University of Portsmouth
School of Computing
Faculty of Technology

A Secure Co-Owned Data Sharing Framework using Fuzzy Group Decision Making and Users Reputation

Gulsum Akkuzu
Supervisor: Dr. Benjamin Aziz

Submitted in part fulfilment of the requirements for the degree of
Doctor of Philosophy at School of Computing at the University of Portsmouth
May 2020

Abstract

The usage of online social networks (OSNs) has become a crucial main activity for individuals in recent days. In OSNs platforms, users are given a space where they can share various types of contents such as, photos, videos, texts, and events. Users are also allowed to share contents of data by including other users ids on the shared content. This type of data is called co-owned data in OSNs. The majority of privacy issues in OSNs platforms are caused by these types of data sharing. Users whose information is leaked, either choose to become unfriend with the user, who leak their privacy, or quit from OSNs platforms, both cases are contradictory to the main OSNs goal. There is a considerable amount of research work done in order to address the privacy issues and proposed solutions. However, privacy issues which originated from co-owned data sharing have still been a problem in OSNs. This research addresses privacy issues, originated from co-owned data sharing processes in OSNs. For instance, users' privacy is still being leaked in Facebook, which is one of the most popular social network, users therefore quit from Facebook or be unfriend with others for protecting themselves. Privacy leakage has a significant effects on people' lives, such as loosing life, breaking up their relationships, be raped. Being unfriend or quitting from social networks are contradictory to main aim of online social networks. This research therefore introduces a framework which makes a balance between co-owned data sharing and privacy preservation.

The developed framework consisted of four main phases which are the contributions of it; (1) a fuzzy logic decision making system, (2) a group decision making system, (3) trust and reputation models, and (4) formal modelling of controlling flow of shared co-owned content. To make these contributions of this theses, this research adopted two methodologies; the mathematical models are developed with adaptation of the scientific methodology and the build methodology is used to implement the developed models in a real world application. The quantitative study was used to model the equations in the developed framework.

In order to evaluate this thesis work, the work was evaluated with a critical comparison with similar works, and the implementation of the developed framework was evaluated with analysis on critical requirements. The main contribution of this thesis is a secure co-owned data sharing framework with mathematical models. The developed framework aims to make a balance between data sharing and privacy preserving in co-owned data sharing processes in OSNs.

The developed framework has provided the most secure co-owned data sharing process with its mathematical models and the systems which compromises the developed mathematical models. It has also shown that data sensitivity depends on the data security features, this means that in the all previous work data sensitivity value was either ignored or decided by someone. However, the person who decides the data sensitivity may not have any idea about it, therefore, this thesis data sensitivity mathematical model solves this issue. All the equations which are used in the developed framework are novel and robust. The robustness are tested based on the developed models' behaviours. The novelty is that there is no mathematical models which can be used in a co-owned data sharing process. They are developed to make not only a trade off between co-owned data sharing and users privacy protection but also make co-owned data processes more secure. The comparison between the developed framework and the similar works in the area has shown that the trade-off between co-owned data sharing and users' privacy protection is possible only if the proposed fuzzy group decision making systems and reputation models are used.

DECLARATION

I here by declare that the thesis entitled “Towards Secure co-owned data sharing by using fuzzy group decision making and reputation systems” submitted by me, for the award of the degree of *Doctor of Philosophy* to University of Portsmouth is a record of work carried out by me under the supervision of Dr. Benjamin Aziz, Designation, School of Computing.

I further declare that the work reported in this thesis has not been submitted and will not be submitted, either in part or in full, for the award of any other degree or diploma in this institute or any other institute or university.

Place: University of Portsmouth

Word Count: 38207

Date: **Signature of the Candidate**

21/05/2020 *Gulsum Akkuzu*

Acknowledgements

I would like to express my sincere gratitude to:

- With immense pleasure and deep sense of gratitude, I wish to express my sincere thanks to my supervisors Dr. Benjamin Aziz and Dr. Mo Adda , School of Computing, University of Portsmouth, without their motivations and continuous encouragements, this research would not have been successfully completed.
- I am grateful to all my colleagues at University of Portsmouth for their helps and many inspiring conversations. I wish to express very special thanks to Dr. Claire Ancient and Dr. Tineke Fitch for their full supports.
- My deepest gratitude to kindhearted, my father Ali Osman Akkuzu,who has taught me the meaning of friendship, hopefulness, and honesty. Also he is the one who has taught me that hardworking, honest living, and honour are the key factors to succeed a goal. It has not only my dream to get my PhD but it has also been his dream. Without him believing in me and supporting me on the time I get down, it would not be possible to complete this thesis.
- To the most ambitious person who was the ultimate source of motivation and inspiration. A strong and gentle soul who taught me to trust in Allah, believe in hard work and that so much could be done with little. To the one who gave up the most important things in her life so that I could take on the most important things in mine. To my role model in this life, my mother Zeynep Akkuzu. Thank you for all the sacrifices you have made.
- Last but not the least, I wish to extend my profound sense of gratitude to Ministry of National Education (TURKEY) for all the sacrifices they made during my research and also providing me with financial, moral support, and encouragement whenever required.

Contents

List of Tables

List of Figures

LIST OF PUBLICATIONS

- Akkuzu, G., Aziz, B., & Adda, M. (2020). Towards Consensus-based Group Decision Making for Co-owned Data Sharing in Online Social Networks. IEEE Access. doi.org/10.1109/ACCESS.2020.2994408

- Akkuzu, G., Aziz, B., and Adda, M. (2020, April). Towards Secure Data Sharing Processes in Online Social Networks. In the 15th International Conference on Software Technologies (ICSOFT 2020).

- Scheidt, N., Akkuzu, G., and Adda, M. (2019,December). Making Decision on Sharing Forensic Data with the Fuzzy Logic Approach. In the 10th IEEE International Conference on Intelligent Systems (IS'20).

- Akkuzu, G., Aziz, B., and Adda, M. (2019, December). Application of Extended IOWA Operator for Making Group Decision on Co-owned Contents in OSNs. In the 10th IEEE International Conference on Intelligent Systems (IS'20).

- Akkuzu, G., Aziz, B., and Adda, M. (2019, October). Advantages of Having Users' Trust and Reputation Values on Data Sharing Process in Online Social Networks. In the Sixth IEEE International Conference on Social Networks Analysis, Management and Security (SNAMS-2019).

- Akkuzu, G., Aziz, B., and Adda, M. (2019, June). A Fuzzy Modelling Approach for Group Decision Making in Social Networks. In International Conference on Business Information Systems (pp. 74-85). Springer, Cham.

- Akkuzu, G., Aziz, B., and Adda, M. (2019, August). Advantages of having users' trust and reputation values on data sharing process in online social networks. In The

Sixth IEEE International Conference on Social Networks Analysis, Management and Security. IEEE.

- Akkuzu, G., Aziz, B., and Adda, M. (2019, January). Fuzzy logic decision based collaborative privacy management framework for online social networks. In 3rd International Workshop on FORmal Methods for Security Engineering: ForSE.

- Akkuzu, G., and Aziz, B. (2019). Data-driven Chinese walls. In 2018 Imperial College Computing Student Workshop (ICCSW 2018). Schloss Dagstuhl-Leibniz-Zentrum fuer Informatik.

List of Acronyms

CRP Consensus Reached Process. 32

CS Computer Science. 42

DBMS Database Management System. 159

EIOWA Extended Induced Ordered Average Weighted. 72

GDM Group Decision Making. 31

MD Micro Distribution. 37

MySQL My Structured Query Language. 159

OSNs Online Social Networks. 4

OWA Ordered Weighted Average. 73

PHP Hypertext Preprocessor. 43

SD Super Distribution. 37

SNGDM Social Network Group Decision Making. 33

Chapter 1

Introduction

The idea of social networks' theories in research was revealed in late 1880s by Ferdinand Tönnies (1887) and Emile Durkheim (1893) respectively. Research on online social networks (OSNs) has taken place in different disciplines such as Psychology, Sociology, and Mathematics. For instance, in the discipline of Psychology, Moreno Moreno (1934) developed a model in which social interactions between people in groups were analysed. In the light of Sociological discipline, structural relations in social groups were analysed by Parsons Parsons (1937) . Prell Prell (2012) analysed OSNs' in terms of mathematical structure with the graph theory and matrices. OSNs were taken into consideration with various perspectives in different disciplines. Above studies on online social networks in different disciplines show that not only computer science researchers have interest in the area but also researchers, who are in the mentioned disciplines, are interested in the area. This means that OSNs can not be squeezed in only computer science area but psychology, mathematics, sociology, and other disciplines.

With the development of the Web 2.0 technologies, the usage of OSNs services has re-

markably increased. According to statistics provided by the statista Social et al. (2019), the most common eight OSNs are given in Table 1.1 along with the number of approximate number of active users in millions. People started to have profiles in OSNs and used these OSNs services for different purposes such as finding friends, sharing contents of data, enjoying the time, shopping, and education. All the activities that people do in OSNs include contents of data, which is either single-owned data or co-owned data. Single-owned data is the type of content in OSNs, which does not contain more than one user's information. Co-owned data is the type of data content, which contains multiple users' information. Each OSN platform on the following table has its own privacy protection mechanisms. These privacy protection mechanisms are called privacy settings which are options that allow OSNs users to control whom should be given permissions to access the shared data. Privacy settings are designed to help OSNs users to close themselves and their data from unknown OSNs users. These privacy settings are mostly designed for single-owned data in those OSNs platforms. However, a co-owned data is not only the type of shared contents in OSNs platforms, also the co-owned data contents are commonly shared in OSNs. Unfortunately, the privacy settings/ privacy policies in current OSNs platforms do not provide adequate privacy protection on co-owned data sharing processes. Therefore, OSNs users have to take precautionary steps themselves on shared co-owned data contents. For example, in Facebook, which is one of the most popular OSN platform, users can remove their tags from the shared content if they do not want their ids to be seen on the shared content.

Table 1.1: Most Popular OSNs

Ranking	Name	Active Monthly Users in Millions
1	Facebook	2.414
2	YouTube	2.000
3	WeChat	1.300
4	Instagram	1.000
5	Tiktok	500
5	Twitter	330
6	Reddit	330
7	LinkedIn	310
8	Pinterest	300

1.1 Motivation and Problem Statement

OSNs platforms are becoming more popular nowadays since they provide an environment where users make social communications, attractive interactions, and share information regardless of their locations. There are currently various social network platforms over the Internet such as Facebook, Instagram, Google+, Twitter, WeChat, Linked-In, etc (see Table 1.1). Facebook is considered as one of the most common online social networking sites, which has approximately two billion monthly active users Social et al. (2019).

As it is mentioned above, such OSNs platforms provide different services to users including sharing different types of content such as videos, photos, and messages. Users are let to upload contents to not only their own spaces but also other users' spaces. The shared contents on other users' spaces may include other people's private information (i.e. *users' ids*). In such data sharing processes, users sometimes leak other users' privacy intentionally but mostly unintentionally. Protecting privacy is one of the crucial concerns that received huge attention in OSNs research area for both theoretical and practical aspects.

Current OSNs allow users to regulate access to the data that is on their own space, however, they can not control or take precaution for content that are shared by others and in-

clude their information. It is most likely to see the leakage of sensitive information while data is being publicised by other users rather that users themselves Hu et al. (2015). Besides that the service providers of OSNs platforms take precaution to prevent data breach, users can also adjust their data access control by using the privacy setting functions implemented in OSNs Xu et al. (2011). Facebook provides individuals with different levels of privacy protection counter-measures in order to decide who is allowed to contact them, who is allowed to see their shared contents, and who is allowed to search them. A privacy policy determines which users are allowed to access the other user's data. OSNs use user relationships and group membership to distinguish both trusted and untrusted users Hu et al. (2011). In summary, OSNs platforms provide a simple access control that allows users to control information on their own spaces, however, users have no rights to control their data that lies on other users spaces.

The most common aim of OSNs' platforms is to keep users account and give users satisfactory results to show them that the privacy leakage on their accounts is a damage and needs protection. Also, OSNs aim to keep encouraging users to share information in OSNs platforms. Commonly used OSNs have preliminary protection mechanism, for instance, *Facebook* allows users to remove tags. However, it can only prevent users' name being seen by other users on the shared content, however the content is still available to the accessors. Original access control policies and privacy settings cannot be changed. Therefore, it is necessary to develop an effective and flexible privacy management framework, which can be adopted by OSNs platforms. In the current OSNs, users sometimes cause privacy issues with sharing co-owned data and users have serious problems in their lives. For example, people loose their relationships, be raped, or even loose their lives. Users either choose to be unfriend with users who leak their privacy or quit from OSNs platforms. Both cases are contrary with the main aim of OSNs platforms, because OSNs

platform's main aim is to bring people together and connect them to each other. Therefore, the developed framework should use a way to punish or award users when they behave in certain ways, especially in co-owned data sharing processes. Also, the developed framework should not only allow users to tag other users but also should allow tagged users to express their opinions for sharing or not sharing the content of data.

This thesis research aims to fill the above gap in the existing literature. It provides a framework that uses fuzzy logic decision making, group decision making, and users' trust and reputation values for secure co-owned data sharing processes in OSNs. Unlike the previous studies in which the decision is taken by only one user, who uploads the content of data to OSNs platforms, without asking co-owners' opinions while the co-owned data is being shared, the proposed framework uses a group decision making in data sharing process in which relevant users opinions are taken into the consideration for taking the decision in the sharing processes. In the proposed framework, the owner who intends to share co-owned data notifies co-owners and allows fuzzy group decision system to make an aggregated group decision based on co-owners' data security choices and data sharing alternatives on co-owned data. The proposed framework also uses the trust and the reputation values in order to make balance between data sharing and privacy protection. This is because current OSNs platforms do not use any mechanisms to punish or award users when they behave in certain ways in co-owned data sharing processes. OSNs users either become unfriend with users who leak their privacy, or quit from OSNs platforms Alsmadi et al. (2016). However, this thesis uses users' trust and reputation values for not only keeping the OSNs' users in OSNs platforms for their satisfactions, but also serves the OSNs main purpose which is to bring people together and make connections among these OSNs' platforms' users.

1.2 Research Goal

This thesis aims to develop a framework which makes co-owned data sharing processes secure. The developed framework uses fuzzy logic-based decision, a consensus-reached group decision making process, and users' trust and reputation values to make secure co-owned data sharing process. The thesis uses a fuzzy-logic based decision making and a group decision making systems in a co-owned data sharing process because none of OSNs platforms use these systems in data sharing process. Group decision making system is required in co-owned data sharing processes if a content of data is related to more than one user. Fuzzy logic-based decision system and group decision system are used to make co-owned data sharing process secure. In order to make the aimed balance between co-owned data sharing and users privacy protection in OSNs, a punishment ans reward system is a need in OSNs. The novelty of this thesis lies on the developed equations and the systems with the systems' variables. The developed framework makes a balance between co-owned data sharing and co-owners privacy violation in co-owned data sharing processes specifically in OSNs and it ensures that the co-owned data sharing process is secure with the developed framework.

1.2.1 Research Questions

In order to accomplish the goal of this thesis, we have developed one main question and four sub-research questions. This thesis achieved its aim by answering the following research questions.

* **[Main Question:]** What is the way to make balance between co-owned data sharing and users' privacy preserving on co-owned data sharing processes?

Due to the privacy issues in OSNs, people have started getting confused whether their shared data violates their privacy or other users leak their privacy. Although there are various settings, which are provided to users by OSNs platforms, to protect their privacy, privacy leakage has still been an issue. There are also new updates in OSNs platforms where users can remove their tags if they do not want their id's being seen on the shared content. Those platforms do not want users to stop sharing contents of data, because that is one of the main aims of OSNs platforms. Users are allowed to remove the tags on shared data, however, the content of shared data is still in OSNs. The aim here is to understand what it is needed in OSNs for protecting users privacy in co-owned data sharing processes, specifically. OSNs should have a new structure/ framework which should make a balance between co-owned data sharing and users' privacy protection in such shared contents of data.

∗ **[Q 1.]** How can we develop a fuzzy logic-based decision making model to make OSNs' co-owned data sharing/ not sharing decisions similar to the real life decision expressions?

Although OSNs reflect people's real lives, the OSNs decision expressions are still Boolean, which is not similar to the real life decision expressions. Fuzzy logic-based decision making expressions are seen much closer to the expressions that are used in people's daily lives. Due to this weak point of OSNs, our aim is to develop a fuzzy logic-based decision model which could not only use *yes* and *no* Boolean expressions but also *maybe* in data sharing decision making process. In the real world, there are various factors which people consider before taking a decision while they share their information with others. These factors are; information sensitivity, acquaintance, reliability of other person. We therefore examine;

∗ **[Q 1.1.]** What are the security features of co-owned data that affect the data sensitivity

value in OSNs?

Which features need to be used to develop co-owned data sensitivity model?

How can we develop the data sensitivity model?

In current OSNs, the data sensitivity value is either ignored or is assumed by the user, who uploads/ shares data in OSNs. However, when a content of data is shared on the Web applications, the data security features are the main criteria for making sure that the data is in the controlled area. Therefore, it is important to know the data security features which make users to get worried about their data sharing process. To do so, we need to analyse related features which have effect on the OSNs co-owned data. It will help us to develop the data sensitivity model. The reason for using data security features to develop the data sensitivity model is explained in Chapter 4.

∗ **[Q 1.2.]** How can we develop a confidence model to show the reliability of a person in a co-owned data sharing process in OSNs?

Current works consider the relation (*i.e. acquaintance*) is the only value for indicating the confidence in a person to take a decision in co-owned data sharing in OSNs. However, in reality, people do not always share their activities and/or secrets with all their acquaintances. For example, a person might share his secrets only with the one he shares his other activities. Therefore, the relation value should not be the only factor to decide the confidence in a person or group of people. There is a need for a confidence model, which should not only take the relations into the consideration but also the data sensitivity.

∗ **[Q 2.]** How can we use group decision making process in co-owned data sharing processes?

Current social network platforms do not use group decision making mechanism

although most of the privacy and security issues are raised from data sharing processes where a group of people are included. The main advantage of group decision mechanisms or/and approaches is to allow decision makers a chance to express their opinions in data sharing process. The group decision making approaches have been applied in different areas, however, it remains unfulfilled in OSNs. The application of group decision making is a need for co-owned data sharing processes in ONSs. The requirements are to know the group members, prepare a set of alternatives, and weight group members' opinions. After fulfilling those requirements, group decision making techniques can be used in OSNs.

* **[Q 2.1.]** Can we apply consensus-reached group decision processes in co-owned data sharing processes in OSNs?

  Co-owned data contents sharing processes should ensure that all peoples' opinions are taken into consideration, who are involved in to the sharing processes. This approach should be used to make sure that the group members take a decision with respect to privacy protection of all groups' members.

* **[Q 3.]** How can we develop reputation model in OSNs?

  Which information is useful to develop reputation model?

  Current OSNs platforms do not use users' reputation values in co-owned data sharing processes. Mostly the reputation systems are used in type of social networks where users buy/sell products. The reputation value is used to analyse whether the buyer/ seller is trusted. However, the reputation values should also be used in co-owned data sharing processes in OSNs in order to show whether a user is trusted or untrusted to make connection or share data. Therefore, our aim is to develop reputation model that can be used in OSNs platforms. To do so, we examine;

* **[Q 3.1.]** How can we model a user's trust in another user in OSNs?

The trust and reputation are taken into the consideration together. Because the reputation is built up with the trust values. In real life, a person's reputation increases if he is a trustworthy user in the community. Therefore, trust model is needed for modelling reputation model.

∗ **[Q 3.2.]** Can we use the trust values in co-owned data sharing processes?

The idea of using trust model in co-owned data sharing processes in OSNs has been discussed by researchers, however, it has not been applied. Therefore, our aim is to make the usage of trust possible in data sharing processes, especially co-owned data sharing processes.

∗ **[Q 4.]** How can shared co-owned data be controlled in OSNs?

How will shared co-owned data be disseminated?

Where will be shared co-owned data diffused to in the future?

Sharing data is not a problem in OSNs however controlling a shared content of data is difficult. It is commonly known that when data is disseminated in OSNs platforms, users do not have control on it anymore. One of the result of not being able to control shared data is to leak other users privacy intentionally or unintentionally.

Figure 1.1 represents the goal of this thesis with the research questions and chapters, which maps the research questions. Four research questions were derived in order to complete the goal of this thesis. Each research question is mapped to chapters which provides the answer for the mapped questions. Some chapters cover more than one research questions.

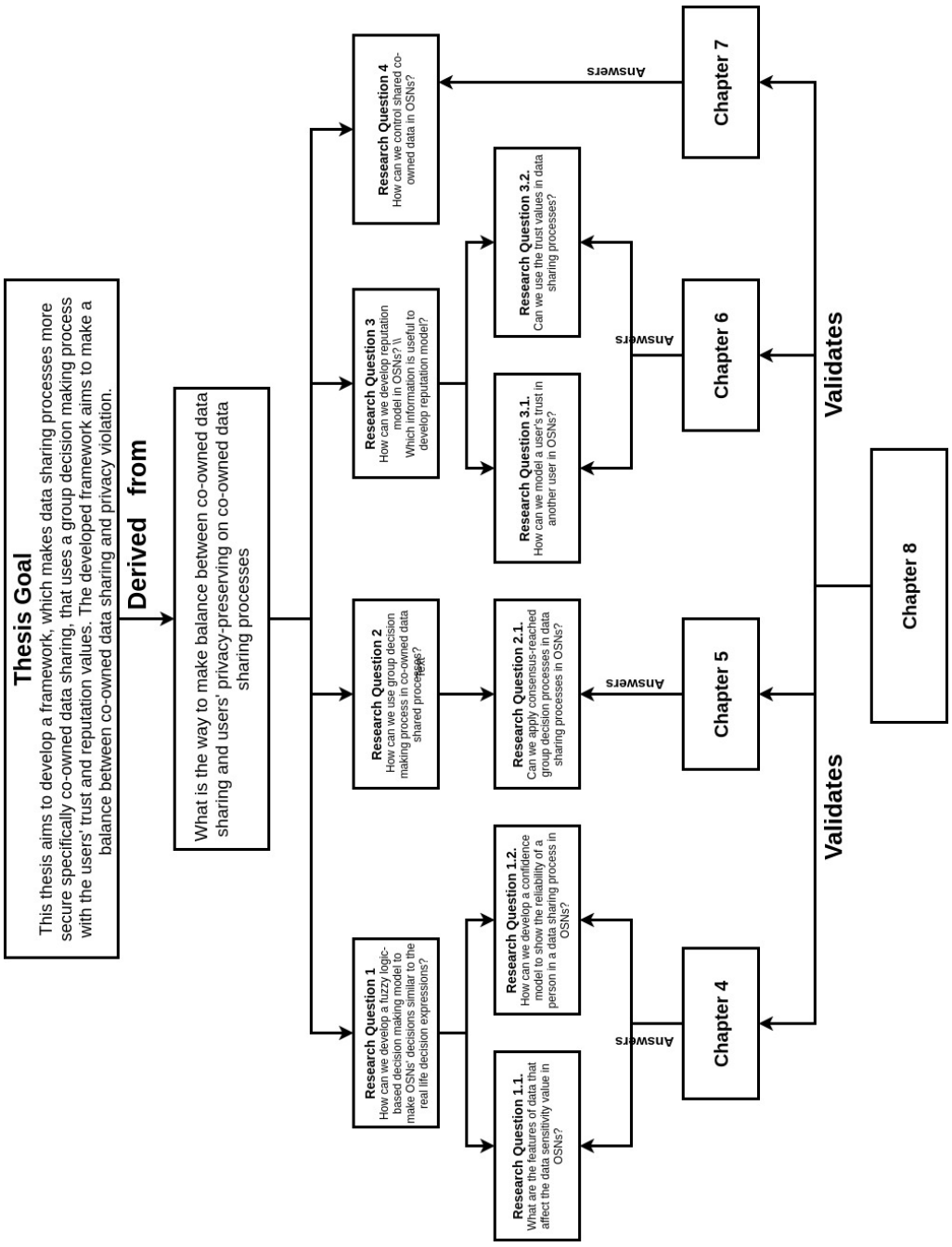

Figure 1.1: Thesis Goal, Research Questions, and Chapters Mapping to the Research Questions

1.3 Road-map of the Thesis

This thesis is structured as follows;

Chapter 1 provides explanations related to the structures of the developed model and the trust values which exist between the users.

Chapter 2 provides a comprehensive literature review of access control management, privacy management, making decision on data sharing processes, trust, and reputation in OSNs.

Chapter 4 proposes a detailed explanation of using fuzzy logic-based decision making in OSNs. This chapter is based on the paper published at ForSE 2019 Akkuzu et al. (2019c).

Chapter 5 introduces a consensus-reached group decision making for OSNs. In addition, it proposes a way of using users' trust values in group decision making processes. We use Extended Induced Weighted Average (EOWA) technique for making the consensus-reached group decision. This chapter is based on the paper published at BISc 2019 Akkuzu et al. (2019d) and on the paper published at IS'20 2020 Akkuzu et al. (2019b).

Chapter 6 proposes a new concept on the trust and reputation values in OSNs. The chapter presents the changes on the reputation with regards to the trust loss and trust gain values. This chapter is based on the paper published at SNAMS2019 Akkuzu et al. (2019a).

Chapter 7 proposes a formal method for system-level modelling of controlling the co-owned data in OSNs platforms. This chapter proposes an approach to control shared co-owned data in OSNs' platforms. The evaluation of the developed model for controlling shared co-owned data is proven in Rodin with refinements and mathematical proves.

Chapter 8 proposes the verification and evaluation of the developed models which are

given in Chapter 4, Chapter 5, Chapter 6, and Chapter 7. Chapter 8 also includes the implementation of the proposed models with an online social web-page named Trusty. This chapter is based on the paper published at ICSOFT 2020 Akkuzu et al. (2020)

Finally, Chapter 9 concludes the work in this thesis and discusses some directions for future research opportunities.

Chapter 2

Literature Review

In the past few years, the usage of OSNs have significantly increased due to the fact that the interaction among users does not rely on their locations Cheung and Lee (2010). In OSNs, users' interactions are mainly based on data sharing which brings privacy issues into the consideration Isdal et al. (2010). Because shared contents tend to include not only user's information, who posts the content, but also other users' information. In such cases, users' privacy issues appear in OSNs ,as the decision is only made by the user who posts the content of data to OSNs platforms.

A wide range of OSNs' privacy issues, including self-disclosure privacy leakage Yang and Tan (2012); Ledbetter et al. (2011), disclosing other users' privacy Krasnova et al. (2010) etc have been studied. In general, researchers focus on the enhancement of privacy policies for users privacy protections in OSNs. All up-to-date research approaches have their strengths and weaknesses Kayes and Iamnitchi (2017). In the literature, there are different approaches researchers have proposed in order to address OSNs privacy issues in OSNs. This chapter, first gives general background information for OSNs and then

gives a critical evaluation on the similar research works in the area.

2.1 Background

This section aims to provide a general background information about OSNs and explanation of the terms used in this work. This section is divided into four categories;

- OSNs and Data Sharing
- Data Ownership in OSNs
- Co-owned Data Sharing Related Issues in OSNs
- Trust Values in OSNs

2.1.1 Online Social Networks and Data Sharing

A social network platform is an abstraction of the representation of peoples' lives in "real" society Li et al. (2017). A social network is denoted as a set of nodes, which are a representation of *people* in real life, connected by a set of edges, which represents *relationship, friendship and tie* Garton et al. (1997). OSNs are web-based services that allow users to do different online activities such as connecting with others, communicating with their connections, sharing contents of data, following other users, and making business Boyd and Ellison (2007). According to the work proposed by Golbeck (2005), OSNs need to cover some requirements in order to meet the definition of OSNs. First of all, they should be accessible with a web browser. Another requirement is that users should be provided with an environment where they can make friendship with other users, or connect to other

users. The last requirement is to make friendship search-able and visible by other users. This definition is open to question because there are web-sites, in which users relationships are not implicit. eBay (`https://www.ebay.co.uk`) could be shown as an example to those websites. OSNs could be categorised based on their utility or functionality Liu (2013). However, the common feature of OSNs is that the communication among users is entirely based on data sharing, regardless of which category OSNs belong to.

Data sharing is one of the main facilities provided by OSNs. OSNs' users are given a chance to share their daily life routines or anything they want to share with other users. Typically in OSNs, a content of data is posted by one user and that user takes the responsibility of managing access of the uploaded data. However, the uploaded data might not belong only to that user, who uploads the content to OSNs, but also different OSNs' users information might be included on it Squicciarini et al. (2010). Unfortunately, this type of data sharing not only have positive effects but also privacy threats on users' either online lives or daily lives Ellison et al. (2007); Acquisti and Gross (2006); Ali et al. (2018). It is important to answer the following questions in order to understand problems in depth; who is the owner of data or what is the ownership of data in OSNs? what are the main reasons of privacy leakage which are related to data sharing in OSNs?

2.1.2 What is Data Ownership in OSNs?

According to Sun et al. (2010), OSNs' data ownership specifies that an OSN user produces, uploads, shares a content of data and manages the accessibility permissions of that content. Xu et al. (2019) Such and Criado (2018) have recently introduced a new view of the definition of data ownership in OSNs. If multiple users are related to a content of data, the ownership does not only belong to the user who shares the data but also to the

users who are related to the content of data.

Definition of Co-owned Data

Each OSNs' data needs to be owned by an OSNs' user. However, some OSNs' contents of data might be owned by multiple users Xu et al. (2018). Co-owned data is considered as a type of data which is uploaded by one user but related to multiple users. The term *co-owned data* is used in this thesis to refer to a content of data which involves different users ids' on it. Figure 2.1 presents a structural view of co-owned data in OSNs. As it is seen in the figure, the content of data which is related to more than one user is called co-owned data. It is important to highlight that related users are named as *owner and Co-owners* in the figure. *Accessors/Viewers* are the group of people who are allowed to access the data after it is being shared.

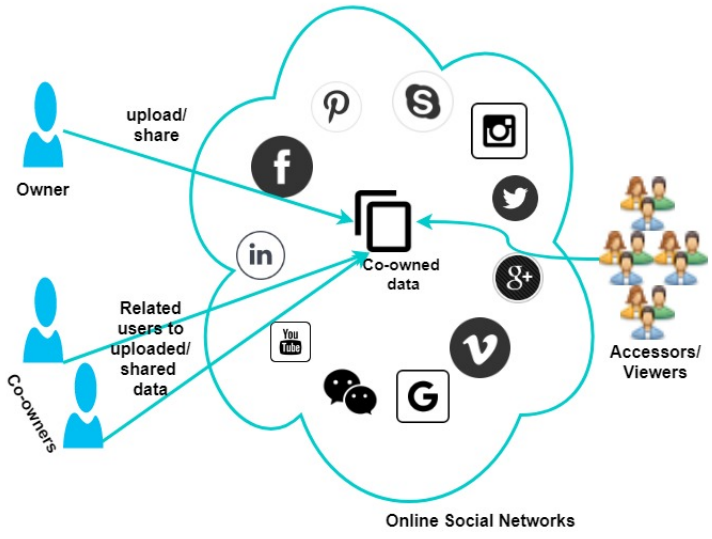

Figure 2.1: Co-owned data and Co-owners Presentation

2.1.3 Co-owned Data Sharing Related Issues in ONSs

According to Krasnova et al. (2010), information disclosure is one of the most common security threats in OSNs. There are different precautions taken by both laws and OSNs platforms in order to prevent privacy leakage issues Nosko et al. (2010). These precautions have helped on self disclosing, however, privacy issues caused by other users still exist in OSNs platforms Li et al. (2015). Co-owned data sharing privacy leakage is one of the current privacy issues in OSNs. Xu et al. (2018) has also addressed the problem in co-owned data sharing processes. He has claimed that the decision on co-owned data sharing processes should not be taken by the user who uploads the data to the platforms, but also by the users (*i.e. co-owners*), who are related to the data. Opinions should be taken whether to share the data or not to share the data. This thesis promotes Xu et al. (2018) idea in which the decision in a co-owned data sharing process should be made by all users who upload or create the data in OSNs.

2.1.4 Trust Values in OSNs

Trust has been discussed in the primary disciplines, such as psychology, sociology, and computer science Buskens (1998); Hörner (2002) concerned with trust relationships. In psychological aspect, the trust is considered to be an individual concept, where the trustee is expected to behave in a positive way to satisfy the trustor Beatty et al. (2011). In sociological respect, trust has conceptual and behavioural aspects, with a dynamic condition since entities' trust values in one another changes over the time Sherchan et al. (2013). Trust definition in computer science is derived from the definitions of psychological and sociological aspects with "a subjective expectation an entity has about another entity's future behaviour" Artz and Gil (2007). This definition of trust in computer science is

mostly associated with online systems since online systems allow interactions between users. However, trust is not a subjective expression and it is difficult to be personalised in OSNs as it is in real life Hamdi et al. (2016). In other words, it is not easy task to quantify trust in OSNs.

In online systems (*i.e. websites*, such as *Amazon* or *eBay*), trust is associated with users' past interactions, which is mainly based on users' feedback whether user behaved in expected way or in an unwanted way Ruohomaa et al. (2007). Caverlee et al. (2008) developed the SocialTrust to support tamper resilient trust establishment in OSNs with three social parameters which are the quality of the user relationships, user behaviour, and personalised feedback. According to *Golbeck (2006)*, the definition of trust in OSNs is a factor that gives information about the people who should share their information and from whom they should accept information. Trust is the unwillingness to be vulnerable on the actions of users towards each others in OSNs Dwyer et al. (2007a). It is used either to confirm a user's identity or to ensure protection of information in OSNs Gong and Wang (2014); Danny et al. (2016). According to Grabner-Kräuter and Bitter (2015), trust is an important aspect to reduce users' uncertainties on users' relationships and information exchanges. This definition can easily be adopted by OSNs platforms since users' relationship exist and the main aim of OSNs is making connection between users and exchanging information among users.

Types of Trust in OSNs

In OSNs, the trust types can be categorised in to three classes; trust between OSNs users, trust between users and the provided online systems, and trust between users and the online service providers Sherchan et al. (2013). The trust between a user and an online system mainly depends on users' satisfaction on various requirements, for example, hav-

ing trust in an online system is a criteria for users Wang and Lu (2010). The trust between members and online service providers is associated with business and marketing fields McLeod and Pippin (2009). Trust that exist between OSNs users depends on the relationship, friendship, or tie value that exists between OSNs' users Coulter and Coulter (2002); Xu et al. (2019).

Trust models have used users interactions *i.e. experiences* as the main source for trust values in OSNs Paradesi et al. (2009). This is because of the fact that users' experiences with each other might affect their future attitudes and behaviours. Starting from this point of trust model view, trust models are mainly developed with users experiences. With this approach, trust has been considered in the literature from the calculative and relational point of view.

Table 2.1 presents research approaches in trust with either relational, calculative, or both perspectives. The table shows that some researchers consider that the trust value is not only a calculative value but also a relational value while others discuss the trust value as either a relational value or a calculative value. Based on both trust definitions, the interactions between users is considered as the main factor for trust values in OSNs. With this respect, in order to asses trust values in OSNs, the trust should be considered from calculative and relational aspects. As we can see from the given table, the trust studies have continued. This shows that trust is an important factor in OSNs platforms.

Table 2.1: Understanding Trust Concept in ONSs from 2010 to Today

Authors	**Calculative Trust** It is the type of trust that aims to maximise trustor's benefits	**Relational Trust** It describes the type of trust in which the interaction between trustor and trustee is the main factor to build the trust value over the time.
Xianget al. (2010)	✗	✓
Podobniket al. (2012)	✓	✓
Al − Oufiet al. (2012)	✗	✓
Chenget al. (2012)	✗	✓
Liet al. (2012)	✓	✗
Zhu (2013)	✓	✓
ZhangandWang (2013)	✗	✓
Riedlet al. (2013)	✗	✓
Choet al. (2014)	✓	✗
Lianget al. (2014)	✗	✓
Fireet al. (2014)	✓	✓
Poppoet al. (2016)	✓	✓
Jianget al. (2016)	✓	✓
Ilicet al. (2016)	✓	✓
DuttaandKumaravel (2016)	✓	✓
Yadavet al. (2019)	✗	✓
SabatiniandSarracino (2019)	✗	✓
Akkuzuet al. (2019*c*)	✓	✓

2.2 Related Work

This section provides a critical review of existing approaches for OSNs' data security and privacy issues, starting from decision making in co-owned data sharing process to controlling the shared co-owned data. Based on the different aspect of privacy issues related to co-owned data sharing and controlling shared co-owned data, the existing research can be divided into categories as follows;

- Making Decision for Sharing Data in ONSs
- Fuzzy Logic-based Decision Making
- Group Decision Making in OSNs
- Trust and Reputation Values in OSNs
- Information Flow Control and Formal Modelling
- Characteristics of Online Social Network

The above research areas have been chosen based on the thesis research questions. In order to answer the research questions and to achieve the thesis aim, the related areas have first been identified. After that, the related works have been critically evaluated.

2.2.1 Making Decision for Sharing Data in ONSs

Making decision in co-owned data sharing processes is a very important action in OSNs because the sharing process might cause privacy issues for other users if the content contains other users' information on it Rahman et al. (2018). In order to resolve the privacy

leakages' issues, which are originated from co-owned data sharing processes in OSNs, different approaches have been proposed.

In the studies of decision making on co-owned data sharing processes in OSNs, Carminati et al. (2006) proposed a rule-based access control mechanism where access policies were based on users' trust levels, types, and depths. This approach provided a basis for new research studies. Gates Gates (2007) proposed a work that addressed the data security requirements by developing a relationship-based privacy requirements model. Squicciarini et al. (2009) proposed a novel approach to the co-owned data sharing issues with the enforcement of privacy policies. It was the first work that used collective privacy decisions where an auctioning algorithm was used to make decision by collecting the choices from co-owners. Hu et al. (2012) developed a similar approach to work in Squicciarini et al. (2009), the proposed model also addressed the privacy issues on co-owned data sharing processes. In their work, the proposed solution did not only collect co-owners' decisions but also used a voting schema for co-owned data sharing decision making processes. The limitation of Squicciarini et al. (2009) work's is that all users opinions are collected but not all opinions are taken into the consideration when the content is shared. They used voting techniques to decide whose decision is taken into the consideration on the sharing process.

Another collaborative privacy management on co-owned data sharing processes in OSNs was proposed by Wishart et al. (2010). In the proposed work, the data owner sets the sharing policy then disseminates the policy to the co-owners. Co-owners are given a chance to make changes in the policy with changes on targeted group and permissions. In their work, collective policy management is applied, however, the proposed work did not address the contradiction on the policies. In parallel, with the development of access control policies for co-owned data in OSNs, access control policies logical implementations were

proposed by Bruns et al. (2012). They introduced the use of hybrid logic for the specification and enforcement of co-owned data sharing decisions in the relationship-based approach to the access controls. The study used the ties *i.e. friendship* in order to make a decision on co-owned data sharing processes. Only users, who have friendship with co-owners, are allowed to have access to the shared co-owned data. The idea of using relationship in co-owned data sharing process is strong while the application of the idea is quite superficial. Because some contents of data might be needed to share not only with friends but also with other users in OSNs.

Co-owned contents of data, especially data which includes tags on it, has been considered as the most potential data to leak users' privacy in OSNs Hu et al. (2011); Such et al. (2017). Both studies have been used to identify the co-owners on the co-owned data sharing processes and make a decision with collaborated access control policies with co-owners, and resolve the conflicts among the entities preferences. Given studies have a general adjustment in each user's personal privacy policy. However, co-owned data sharing requires fine-grained adjustment in every co-owned data sharing process.

In summary, the above studies proposed models making decision to solve problems in privacy disclosing issues because of co-owned data sharing processes. However, proposed studies have not only been weak to solve the privacy problems but also have raised issues on privacy policies conflict. With the aim of detecting and solving policy conflicts on collaborative privacy management approaches and developing the new approaches to solve the privacy leakage, new approaches have continually been developed.

2.2.2 Collective Privacy Management in OSNs

Collective privacy management on co-owned data in OSNs has been studied by researchers. This section gives research studies with their proposed approaches.

Squicciarini et al. (2009) has addressed the problem of privacy management in co-owned data sharing processes in OSNs. They used *Clarke-Tax* mechanism to collect the privacy preferences and then used the *Game Theory* technique for the evaluation. The problem in their work is that not all co-owners' opinions were taken and evaluated.

Wishart et al.Wishart et al. (2010) has provided a collaborative privacy policy authoring in the context of social networking. They allowed the originator of the data to specify policies for the content, however, the work does not consider co-owners' privacy policy specifications.

Hu Hu et al. (2015) has proposed a collaborative management on co-owned data sharing processes in OSNs. It is a very simple and flexible mechanism. Although the mechanism provides conflict resolution that considers both the privacy risk and data sharing loss. This study does not have any control if privacy loss happens.

Suvitha Suvitha.D (2014) has formulated a multiparty access control and policies. He used voting mechanism for making decision on co-owned data. Collaborative privacy management issue might be described as a mother of the privacy conflicts. Therefore, it is an inevitable point to be involved while the co-privacy management of shared data is considered.

Joseph Joseph (2014) has proposed a solution for privacy risk and sharing loss for collaborative data sharing in online social network. The work proposes an algorithm to identify conflict segments in accessor space. A framework was developed for protecting and se-

curing co-owned data for public OSN by Shaukat et al. Ali et al. (2017). They pointed that the privacy risk is seen not only from unauthorised users but also from the OSNs service providers. They used cartographic-based technique in their framework to overcome privacy concerns.

Recently, a work has been proposed to address collaborative privacy management with an agent-model Ulusoy (2018). He has proposed to modify Clarke-Tax mechanism that was used in Squicciarini et al. (2009). Du et al, proposed an evolutionary game model that analyses how a user's data privacy protection is affected by other users' privacy decisions Du et al. (2018).

Briefly, in all the above mentioned studies, stake-holders' (*i.e. co-owners*) preferences were collected by a mediator (*i.e. third party or OSNs platform*) and used the technique proposed in each study' for applying the collaborative privacy management on co-owned data sharing processes in OSNs. However, none of the above studies considered using the group decision making techniques and also did not consider the punishing or awarding of the owner in co-owned data sharing processes if the owner behaves in a good way or bad way in the sharing process.

2.2.3 Fuzzy Logic-based Decision Making

The deficiency of OSNs' platforms is to provide Boolean decision expressions (*yes/no, share/not share*) in the data sharing processes. However, real-life problems and human approaches are not bivalent Tong and Bonissone (1980). In order to overcome the above requirements in the real life decision expressions, fuzzy logic and fuzzy sets were introduced by Zadeh Zadeh (2008). The crucial point of fuzzy logic is that it is based on fuzzy sets while Boolean logic is based on classic sets Sanayei et al. (2010). In a fuzzy set,

there is no predefined boundary between objects, therefore, each element of the set is associated with a value which indicates to what degree the element is a member of the set. This value ranges [0,1] in which *0 indicates the minimum degree of membership, 1 indicates the maximum degree of membership, and intermediate degrees indicate 'partial' membership* Bevilacqua et al. (2006). It operates with blurry boundaries and uncertain concepts. Problems can be reflected with the degree of truth or falsity, for example, the expression, my decision is yes, could be 100% yes if there are no questions and doubts in the decision, 80% yes if there are some doubts in the decision, 50% yes if the decision is not certain at all, and 0% yes if the decision is no.

Decision making is an important and challenging process because uncertainties and doubts create difficulties for decision makers. The reason is the subjectivity of the expression of natural language. Therefore, researchers have focused to develop more accurate, mathematical, and specialist decision making systems, such as expert systems, neural networks, fuzzy logic, and machine learning Das (2016); Yadav et al. (2018); Sanayei et al. (2010); Yager (2018). Fuzzy sets theory was introduced to solve uncertainties, vagueness, and subjectivity of human reasoning. It also helps to express linguistic values in decision making processes Zadeh (2008); Abdullah (2013). Fuzzy systems have been applied to address decision making problems Carlsson and Fullér (1996); Wang and Chang (2007); Liu et al. (2018), by offering a mathematical way to apply vague preferences. They have been more successful than traditional expert systems for handling uncertainty information in decision making systems Das (2016). In fuzzy systems, there are two approaches: the expert-knowledge-based approach and the data-driven approach Adoko et al. (2013); Chen and Chen (2002).

Expert-knowledge-based approaches require human expert to define rules, and a strong background to define rules for a fuzzy system Hüllermeier (2015). However, when data

is available, fuzzy systems can be constructed by various techniques, such as, clustering, classification, or other techniques. These two approaches have drawbacks and benefits, for example, the expert-knowledge-based approach provides a set of linguistic terms to make explicit fuzzy rules in the system. It helps to interpret rules easily. However, in the data-driven approach, an interpretation of rules is difficult but rules are more general. This means that there are almost no redundant, missing, and unnecessary rules Adoko et al. (2013). As a result, both approaches have been applied to solve real-world problems.

The challenges of using fuzzy logic-based decision making approaches in OSNs have been addressed by Cabrerizo et al. (2015). Dunbar (2016) has also addressed the deficiency of decision expressions in OSNs. Most of the fuzzy logic modelling approaches for OSNs co-owned data sharing focus on group decision making process. With respect to this, the thesis use fuzzy logic-based decision expressions in a group decision making process.

2.2.4 Group Decision Making in OSNs

Group Decision Making (GDM) is a process where the final decision is no longer attributable to a single user. In a GDM process, mostly a decision maker takes the responsibility of evolving other decision makers' opinions and releases the final group decision Liang et al. (2016). Group decision making is an important and challenging process because it includes decision makers' doubts, problems, and uncertainties Liang et al. (2017). Therefore, finding appropriate ways to help decision makers is one of the key and critical point in a GDM process. Thirumalai and Senthilkumar (2017) has proposed a fuzzy model to resolve the group decision making problems in business areas. The proposed approach uses membership and non-membership attributes to make the group decision.

Fuzzy systems have been used to solve the group decision making problems in OSNs Liang et al. (2017). GDM processes are efficient approaches to tackle decision making issues when the decision making process involves a group of people. Eventually, a GDM process usually aims to choose the best alternative from a set of alternatives.

Traditionally, there are two processes in GDM; one is consensus reaching process (CRP) and the other one is selection process Hochbaum and Levin (2006). When a consensus-based decision is reached by group members, a selection process is applied Roubens (1997). CRP is considered as the most important step for GDM because it indicates that the decision makers' opinions are re-evaluated to reach the final decision Dong et al. (2018). The consensus process is considered as a repetitive process in which the decision makers may change their opinions on the alternative set based on the advice given by the moderator (third party) Herrera-Viedma et al. (2017). The advise system includes a feedback mechanism to reduce the inconsistencies in the knowledge provided by decision makers Dong et al. (2015). The consensus reaching approaches have been quite productive approaches in OSNs because OSNs provide an environment where people can communicate to each other.

With the rapid growth of OSNs' usage and continued privacy issues in decision making processes within OSNs, these decision making problems have attracted researchers attentions from different perspectives Alonso et al. (2013); Li et al. (2014); Li and Lai (2014); Recio-García et al. (2013). Tindale and Winget (2019) have shown that OSNs include the real-time communications. The contents of online shared data requires GDM processes because the decision should be as close as to the real-life decisions. OSNs provide relationship among users, GDM process requires a social interaction between users Pérez et al. (2016). The first social network consensus reaching approach was proposed by Alonso et al. (2013), which included a feedback mechanism and delegation mech-

anism for enhancing the consensus solution. This approach has just attempted to use a consensus-reached decision making system in OSNs, however, the proposed work has not been applied.

CRPs have continually been improved by researchers day by day with either new models or with its applications. Li et al. (2013) has proposed a generalisation of the Deffuant-Weisbuch model and studied opinion dynamics in a connected network according to the hard-interaction model and the strategic interaction model. They have showed how a required situation guarantees opinion aggregation in the hard interaction model and also showed how opinion formation processes are affected by the individual incentives behind interactions. The work has mainly focused to show the importance of CRP and GDM in OSNs and indicates the usability of OSNs relationship values in GDM processes.

Choosing the best parameter for the feedback mechanism has attracted researchers' attentions during the recent years Wu et al. (2018), Wu et al. (2015b). *Wu et al.* have proposed a recent work to minimise the changes on decision makers opinions and reduce the cost of feedback to reach the consensus for group decision making and have also expressed the trust values with linguistic terms. The usage of the trust values has been one of the resolution for inconsistency of the decision makers. The importance of the trust values has been addressed by Herrera-Viedma et al. (2007), Urena et al. (2019). It has been the first work that applied the trust values to reach satisfied consensus-based group decision in social network group decision making processes SNGDM. Wu et al. (2015a) has presented a new consensus approach that includes a trust based estimation method and an illustrative consensus aggregation model. In order to determine users' weights and to estimate the unknown evaluation values, a relative trust score is used in the proposed work. Labella et al. (2017) have proposed a work which has aimed to resolve the problems in GDM by comparing different GDM models by means of the advantages and disadvantages of the

models.

The advantages of the GDM and CRP in OSNs have been discussed in above mentioned work. OSNs have an environment in which decision makers can communicate with each other in order to make the best decision among alternatives given to decision makers. In summary, GDM approaches are applied to the situations in which group decision makers come together to solve the problem. With this respect, OSNs co-owned data sharing process requires GDM approach since the shared data might cause a privacy problem.

2.2.5 Trust and Reputation Values in OSNs

Trust and reputation are taken together into the consideration since assessment of trust is the main factor to develop the reputation value Sherchan et al. (2013). The common and simple examples to differentiate trust and reputation are *"I trust you because of your good reputation"/ "I trust you despite your bad reputation"* Jøsang et al. (2007). Trust and reputation are used for evaluating an entity's trustworthiness, therefore trust and reputation systems provide a choice to select trusted services, entities, applications and users in OSNs Wang and Vassileva (2007); Sherchan et al. (2013); Azer et al. (2008); Momani and Challa (2010); Yu and Wang (2010); Joinson et al. (2008). *Caverlee et al. (2008) et al.* use the real life trust and reputation perception, meaning that if someone's reputation is bad, then that user will be considered as untrusted user. Their claim is that users' bad behaviours affect their reputation, thereby malicious users can be realised by other users with their reputation. The first part of that claim can be supported because the reputation value is built up by looking at someone's good and bad behaviours and the reputation value can help others to have some opinions about the person. However, the other part of the claim is open to discussion, as the reputation should be assessed environmentally. For

example, a person can have a bad reputation in an area while s/he can be well reputed in other areas.

In OSNs, the aim of having the reputations systems is to have an opinion about a user's future actions by looking at his/her past behaviours. It basically collects users' experiences about the other users and brings the possibility of detecting improper peers Jensen et al. (2002); Hogg and Adamic (2004); Mehra et al. (2006); Wasko et al. (2005); Ruohomaa et al. (2007). In order to build the reputation model's feedback of other peers, a specific peer is used as a utility function which reflects the satisfaction of a peer experiences after using a service or consuming a product Arenas et al. (2010). There are few studies, which have pointed the usage of the reputation in different concepts for online social networks Paul et al. (2012); El Marrakchi et al. (2015); Alsmadi et al. (2016); Xu et al. (2018). The need of reputation values in OSNs has been proposed by *Paul et al. (2012)*. They claim that OSNs' users need to have an explicit information about other users. Researchers then have started to formalise reputation models for OSNs users El Marrakchi et al. (2015). Reputation measuring has been built upon a user's interaction in OSNs Alsmadi et al. (2016). The effectiveness of trust on reputation modelling has been discussed in Xu et al. (2018); Schweitzer et al. (2019). According to *Schweitzer et al. (2019)*, not having an explicit information on users' profiles about their past interactions is one of the crucial reasons for users being connected or not being connected with other users in OSNs. Having explicit reputation values on OSNs users' accounts or profiles have been seen challenging because of difficulty about defining the feedback factors.

In summary, the above mentioned works indicate the idea of having reputation values in OSNs. However, there is only one work, which was proposed by Xu et al. (2018), has considered to use the reputation values in OSNs data sharing processes. As it is abovementioned that the reason for not having reputation values in OSNs is a challenging task to

identify the feedback values in order to calculate the reputation. It requires mathematical modelling and determining what factors can be used for reputation values calculation. In order to fill those gaps, this thesis first identifies what factors could be used to calculate the reputation values, then it develops models for calculating reputation values in OSNs data sharing processes.

2.2.6 Information Flow Control and Formal Modelling

With the increment usage of the Internet, the security concerns on shared information have become more important and common Krohn et al. (2007). Researcher have started to work for improving the security of shared information with different approaches. Security policies were proposed to control information flow such as Lattice model and mandatory access control policies Puthal (2018). Information flow control is related to security policies in a system in order to make sure that information does not flow to unwanted areas, however, security policies do not focus on the content of information. Therefore, content dependent information flow control approach has been proposed by Nielson and Nielson (2017). The proposed work claims that the flow of information needs to be controlled based on contents. This thesis supports the content dependent information flow control in OSNs. In order to control the content flow, the shared content needs to have some deterministic features.

As it is aforementioned, the modelling and analysis of OSNs is not a new idea. It has been under-research in many aspects. OSNs' formalisation and modelling are usually done with the graph theory Marin and Wellman (2011). OSNs are considered as a set of nodes and edges that tie one node to another. Nodes and edges are used to define OSNs Hanneman and Riddle (2005). Analysing the trace of data flow among nodes is

linked to relationships. If two nodes have edges between them, then the accessibility of the content is allowed Ali et al. (2007); Bhargava et al. (2012); Fong and Siahaan (2011); Liben-Nowell and Kleinberg (2008). There are various proposed models for information flow control in OSNs in which the trust values between nodes are used Lu et al. (2006); Jiang et al. (2015). Akkuzu et al. Akkuzu et al. (2019a) have recently introduced a new approach for secure data sharing processes in OSNs. They suggest to use not only the users trust values but also users' reputation values. The strong point of this work is that it has aimed to give an indicative information on users' profiles.

Another proposed method for controlling information flow is group-centric models in which users' authorisation in a group membership is used Krishnan et al. (2007). They used Super Distribution (SD) and Micro Distribution (MD) for providing a secure data sharing environment. Authors in Zdancewic and Myers (2001) introduced a new model for controlling information flow in OSNs with mutual distrust and decentralised authority. A new OSN was introduced by Baden et al. Baden et al. (2009) where users decide who can have access to their information.

As it is above mentioned, controlling shared contents is a crucial concern in OSNs. It is possible to control the contents of data for the first targeted group, however, it is not easy to control the shared data when it is started to flow in OSNs.

Event -B Abrial (2010) is an advanced model of the B method Abrial and Abrial (2005), allows users to create formal method for modelling complete systems. Event-B is an action based modelling language; the system behaves in a certain way when an action happens Rivera et al. (2017). There are two constructs in the Event-B; the context and the machine. The context contains carrier sets, constants, axioms, and theorems which is the static part of a model. The machine contains the dynamic part of a model such as invariants, variables, variants, and events. The states of the machine are defined with

variables. Events includes the changes that occur in the variables. Each event involves a guard G and an action S, where the guard states necessary conditions under which event might occur, and the action describes how the state variables evolve when the event occurs. The correctness of an Event-B model is defined by an *invariant* property which every state in the system must satisfy. So, every event in the system must be shown to preserve this invariant. In order to verify this requirement, proof obligations have been defined. Another important feature in the Event-B is the refinement, which transforms abstract and non-deterministic specification into a concrete and deterministic system that preserves the functionality of the original specification.In Event-B, an event is represented by the following term;

$$\mathrm{e} \mathrel{\hat{=}} \textbf{EVENT } e \textbf{ WHEN } G \textbf{ THEN } S \textbf{ END} \quad ,$$

where e is the representation of event parameters, G presents the guard, which is the conjunction of one ore more predicates and S stands for the action.

The aim of formal methods modelling in this thesis is to model the control of shared co-owned data flow formally. Furthermore, the purpose of applying the formal methods modelling in this thesis is to solve the flow of shared co-owned data at the requirements and specifications. Hereby, it can show the importance of controlling the shared co-owned data from the security point of view.

2.2.7 Characteristics of Online Social Network

According to Buchmann (2013), OSNs are categorised into two major parameters which are users and data. Zhang and Guo also claimed that the most important parameter in OSNs' platforms is a node (*i.e. user*) and its actions Zhang and Guo (2014). The benefit of OSNs is based on the number of the users on it and the number of data is shared on it

Proudfoot et al. (2018). After the specification of OSNs characteristics and its benefit, the security concern in OSNs' platforms was taken into the consideration Alqatawna et al. (2017). *Alqatawna et al.* discussed the main security issues in OSNs platforms, for example, threats on a data sharing process was pointed by them Alqatawna et al. (2017). They showed Facebook as an example for discussing its weak and strong points; although it was claimed that Facebook uses strong privacy policies for protecting users' privacy, users still have privacy concerns and they quit from the platform.

There are main requirements which are needed to be used in a typical OSN platform, such as log in, profile settings, search friends, shares, likes, and log out Amato et al. (2018). Any social networking site which meet the specified requirements is considered as an online social network. Therefore, there are many online social network on the Internet, such as Facebook, Twitter, Instagram, and YouTube. However, it does not mean that all online social network have a secure data sharing environment for users. There is a need in the area of OSNs which is a structural framework that should be able to make a balance users' privacy preserving and data sharing. In order to fill this gap in the area, we developed an online social network in which data sharing process is more secure and there is a way to make a trade-off between data sharing and users privacy preserving.

2.3 Conclusion

OSNs have become a cultural phenomenon for people as Web technologies developed. The increment on usage of OSNs has also affected information sharing. This increment has encouraged users to build more relationships and share more information with each other in OSNs platforms. As a result, OSNs' users have shared their personal information or contents of data with either their contacts or public (*all users in an OSNs' platform*).

Those shared contents of data sometimes do not include only a single user's information but also multiple users' information. In many cases, those types of data sharing have caused information exposure to unwanted users or privacy issues in OSNs. As a result, users unfriend the other users, who exploit their personal information to unwanted users, or quit from OSNs platforms. However, being unfriend or quitting from OSNs is contrary to the main aim of OSNs. In order to protect privacy leakages because of this type data sharing in OSNs, researchers have proposed different approaches, which are discussed in above sections. We have provided a comprehensive overview of various approaches on how to have a secure co-owned data sharing process in OSNs platform and how to make a balance between co-owned data sharing and users privacy protection.

Although previous works have made significant contributions to the literature in order to have more secure co-owned data sharing processes in OSNs, there are still gaps to be filled in the literature. For example, most of the works tend to assume that the data sensitivity value is single-handed for co-owned data and therefore ignore other users' security and/ privacy concerns on the co-owned data sharing processes. However, the co-owned data could be non-sensitive for the owner while it is very sensitive for co-owners. There is also no work which applies group decision making techniques in co-owned data sharing processes in OSNs although most of privacy leakages are caused by sharing co-owned data, which includes group of people on it. None of the work in the literature has applied a reward or punishment system in co-owned data sharing processes based on users behaviours. Another lack of the previous works is that none of the previous works have used a formal modelling to show that there is no missing point in their proposed work. Lastly, any of the previous theoretical approaches have been applied with a practical concept.

In this research, we therefore have developed a framework which aims to make a balance

between co-owned data sharing and privacy protection in OSNs and make co-owned data sharing process more secure. Developed framework uses fuzzy group decision making and users reputation values in co-owned data sharing processes in OSNs. It also has formal modelling of the developed framework with an implementation as a practical part of it.

Chapter 3

Research Methodology and Preliminaries

This section first introduces the research methodology used in this thesis. Second, it provides a structural view of the developed framework. It also gives terminologies that are used in this thesis.

3.1 Methodology

A research methodology can be defined as the technique or specified procedure which is used to identify the'; followed way in order to solve the identified research problem. In Computer Science (CS), the research methodologies that are used to tackle with the research problem are diverse. Elio et al. (2011) discussed several types (e.g. from *formal methodology* to *model methodology*) of research methods in the *CS* field with respect to tackle research questions within the discipline. It has also suggested that several method-

ologies can be used for a single research question which means that there is no restriction for a research to use a single methodology.

In this thesis, the scientific methodology and the build methodology have been adopted in order to achieve the goal of the work. The scientific methodology requires certain steps for a research being completed Dodig-Crnkovic (2002). The steps of scientific method are as follows; 1) Pose research questions by using the context of existing literature works. This step is completed in Chapter 2 in this thesis. 2) Formulate a tentative answer for defined research questions. 3) Formulate models and deduce consequences. 4) Test the developed models until the agreement is obtained. The second, third and fourth step of the method are covered in Chapter 4, Chapter 5, Chapter 6, and Chapter 7 in this thesis. 5) Combine the developed models for developing a framework which needs to cover all the research questions. This thesis has followed the scientific methodology. First of all, the research questions have been defined in order to fill the research gap, which was discovered with observation in privacy issues in OSNs. Then, the ways for answering the research questions have been defined with the development of the models. Finally, the developed models have been merged together in order to develop a framework which aims to make a balance between co-owned data sharing and co-owners privacy protection.

This thesis has also used the build methodology for implementing all the developed models in a software. In the build methodology, there are four steps Elio et al. (2011); designing the software, using/ reusing components, choosing a suitable programming language for building the software, and testing the system whether it works with the developed models or not. *Hypertext Pre-processor: PHP* has been chosen to implement the developed models in a real world web application. In order to test the usability and efficiency of the developed models in the implemented online web-site, two questionnaires were conducted which have been located in the end of each co-owned data sharing process.

Implementing the developed models in an online social network has given a chance to evaluate the developed models with users interactions. Chapter 8 is the part that used build methodology in this thesis.

Figure 3.1 presents the methodological steps which are taken to accomplish this thesis. Taken steps in the figure are also the guide for answering research questions.

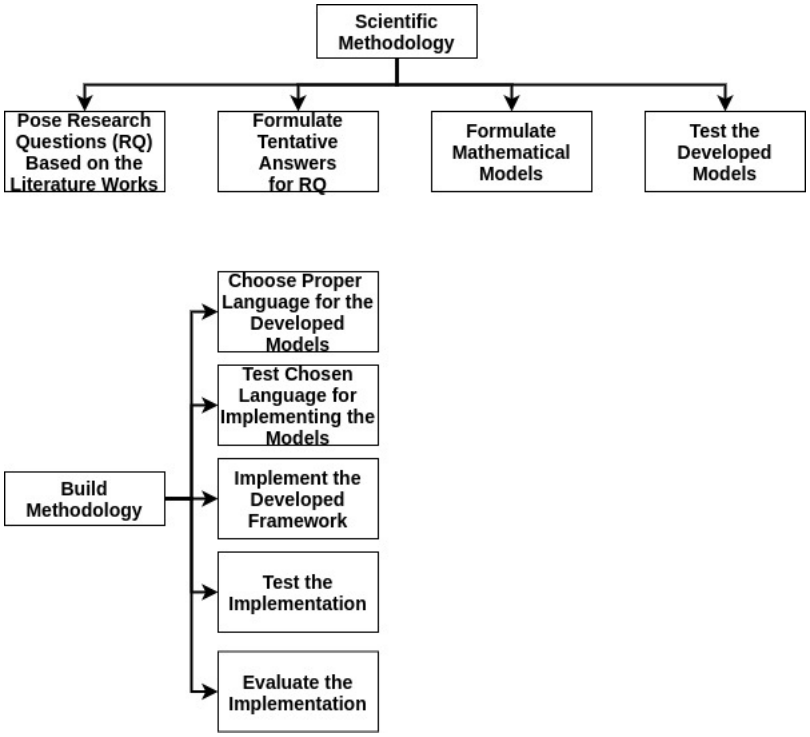

Figure 3.1: Methodology Steps

Related works in the area helped us to chose this thesis research method and develop its research questions (see Chapter 2). Chapter 4 and Chapter 5 cover fuzzy logic-based decision system and group decision making system, respectively. Chapter 6 covers a reputation system with the use of trust models. Chapter 7 covers the formal modelling of the above chapters, this chapter proves that the framework is completed and ready for implementation. All the above chapters are the backbone of this thesis because they include all mathematical models and systems that are needed to make a balance between co-owned

data sharing and users privacy protection. Lastly, Chapter 8 is the part in which build methodology is used from its start to its end. This chapter presents that the framework is not only theoretical structure but also practical.

3.1.1 Preliminaries

The aim of this thesis is to develop a framework, which uses a consensus-reached decision with a fuzzy logic decision and users' trust and reputation values. This introduces a way to make a balance between co-owned data sharing and preserving users' privacy in OSNs' platforms. This chapter gives the structure of the developed co-owned data sharing framework and the structure of the trust values which exist between the users.

The framework's structure is given in Figure 3.2. The structure of the trust values that exist between the users is given in Section 3.1.3.

Table 3.1: Terminologies of this Thesis

Terminology	**Definition**
Owner	the user who uploads the content that includes other users information on it
Co-owner	users whose information is included on the content that was uploaded by a user in OSNs
Co-owned data	The content includes multiple users' information on the content needs be controlled by multiple users

3.1.2 The Structure of the Developed Framework

Figure 3.2 shows the structure of the developed framework of the thesis. In the figure, each part of the framework is specified with the related chapters. Table 3.2 explains who is responsible for what in the framework. Table 3.1 and Table 3.2 present terminologies

of this thesis and roles which are related to the given terminologies, respectively. Table 3.1 presents the main terminologies that are used from the beginning to end of this thesis. Table3.2 shows the roles of the developed framework and the related activities to each role. The owner and the co-owner appear in both tables but they have different explanation on each table as it is above mentioned (Please see related rows and columns).

Table 3.2: Roles and Activities of Roles

Who	**What**
Owner	The owner is responsible to upload/create the content of data Specify the targeted group for the content Choose to notify **co-owners** Wait until co-owners make a consensus-reached group decision Take the final decision Decide whether to control or not to control flow of co-owned data
Co-owner	take the responsibility of giving preferences in CIAPP features take the responsibility to choose alternatives from the supported alternative set
The System	Notify selected co-owner with the contents of co-owned data and the targeted group for data Give co-owners CIAPP features and Fuzzy alternative set Check consistency of DEI-DEO Notify owner whether consensus is reached or not Give recommendation to co-owners Allow owner to make the final decision Control flow of shared data

3.1.3 The Structural Representation of the Trust Among Users

Figure 3.3 is an illustration of the trust values that exists between users in OSNs platforms. The system assigns a starting trust value τ to users when any two users become friends. In other words, when a relationship values appears between any two users, trust values between two users are assigned. The trust values are dynamic values which are changed in the end of co-owner data sharing processes. Let us think that two users *user i* u_i and

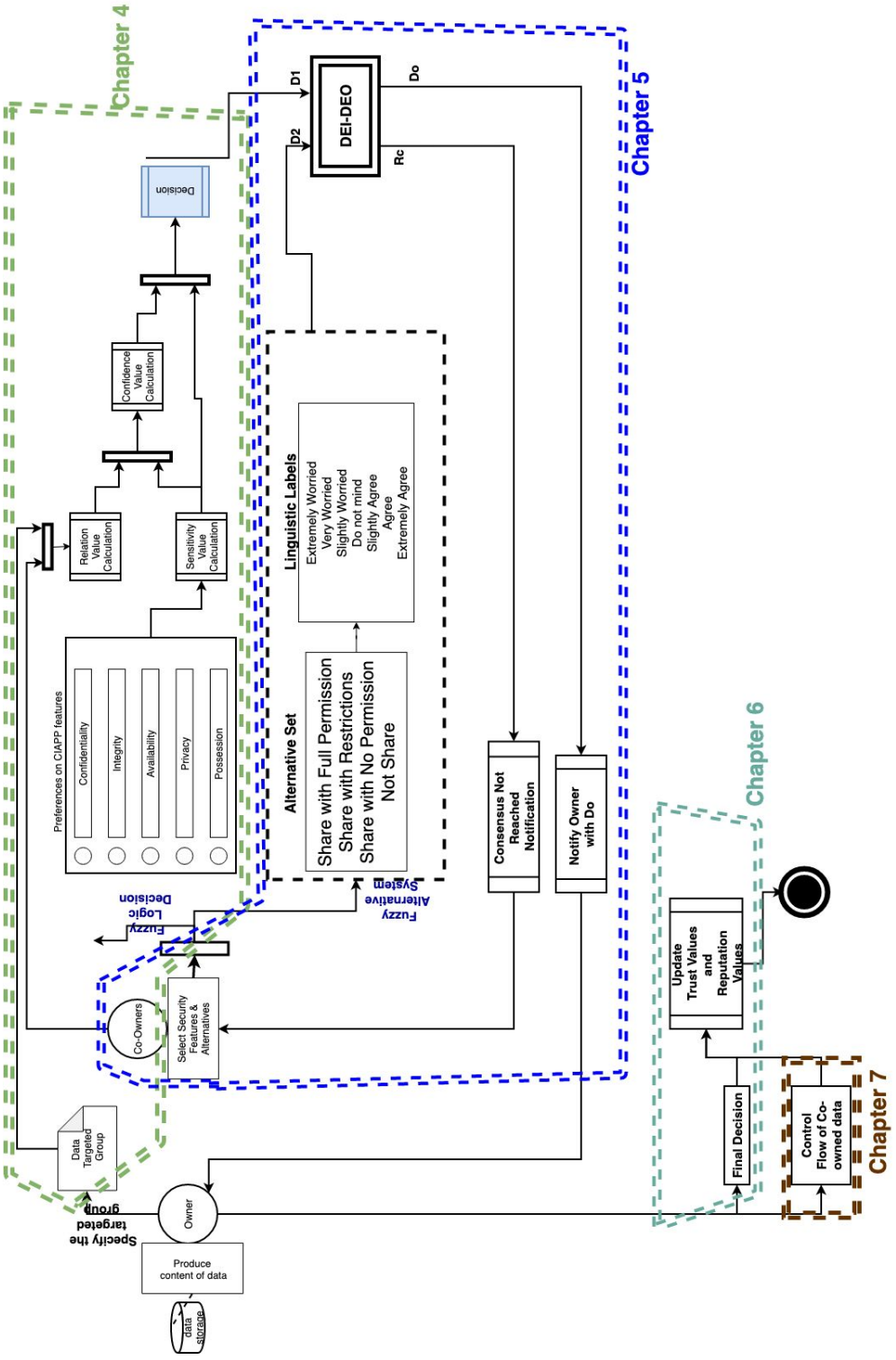

Figure 3.2: The Structure of the Developed Framework

user l u_l are connected to each other with friendship tie, the system immediately assigns τ values for user i's trust in user l τ_{ui-ul} and user l's trust in user i τ_{ul-ui}. As it can be understood that trust values between users are directed from user to user. The detailed explanation of trust values and calculating the trust values between users are given in Chapter 6. The equation and the behaviour of the trust model is also shown in Chapter 6.

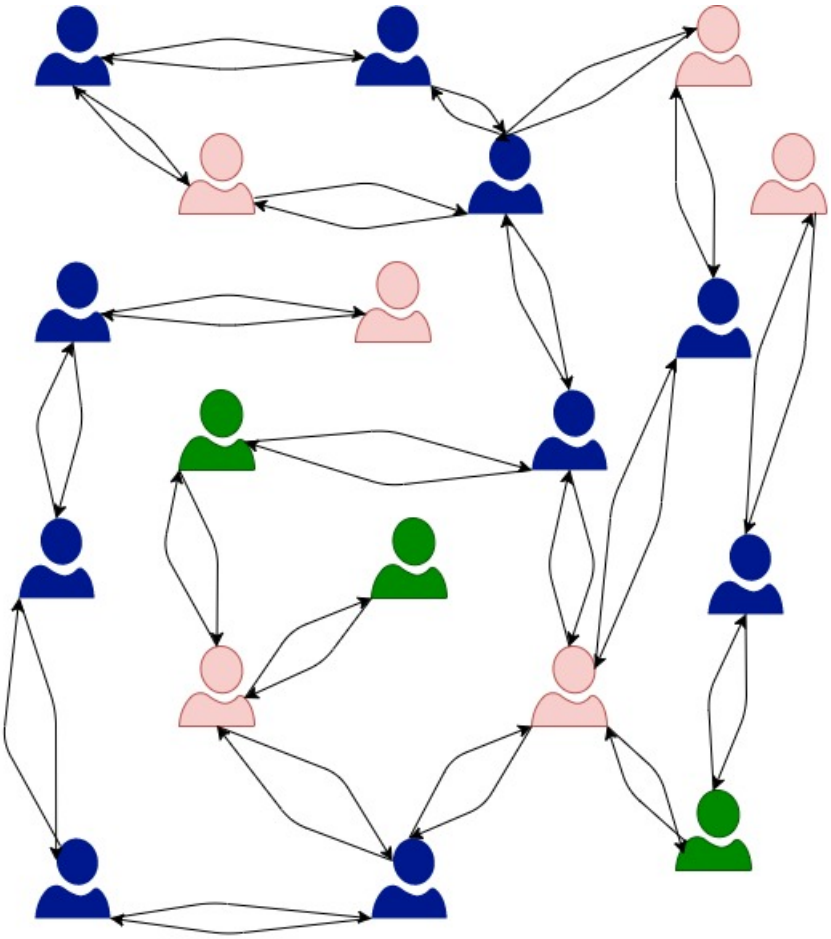

Figure 3.3: The Structure of the Trust Values Between Users

3.2 Details of a complete picture of the framework

The main aim of this thesis is to make a balance between co-owned data sharing and users' privacy protection. To make the balance, we used a fuzzy logic-based decision making system, a fuzzy group decision making system, reputation system, and a formal system to control flow of shared co-owned data.

Figure 3.4 represents aggregated parts of the framework. Given parts in the figure are connected to each other for achieving the aim of this thesis. As it is showed in the figure, fuzzy logic-based decision system and fuzzy group decision system are in co-owned data sharing process part. The control flow of shared co-owned data and the reputation system are in the users privacy protection part. Fuzzy systems work in parallel. When data sharing process is completed with the completion of both fuzzy systems, the next process is started and completed in the developed framework. Fuzzy systems are connected to each others in the framework because it is important to make a convenient decision from these fuzzy systems. The same approach is applied in the users privacy protection part with a punishment/award system and restriction on the future flow of data.

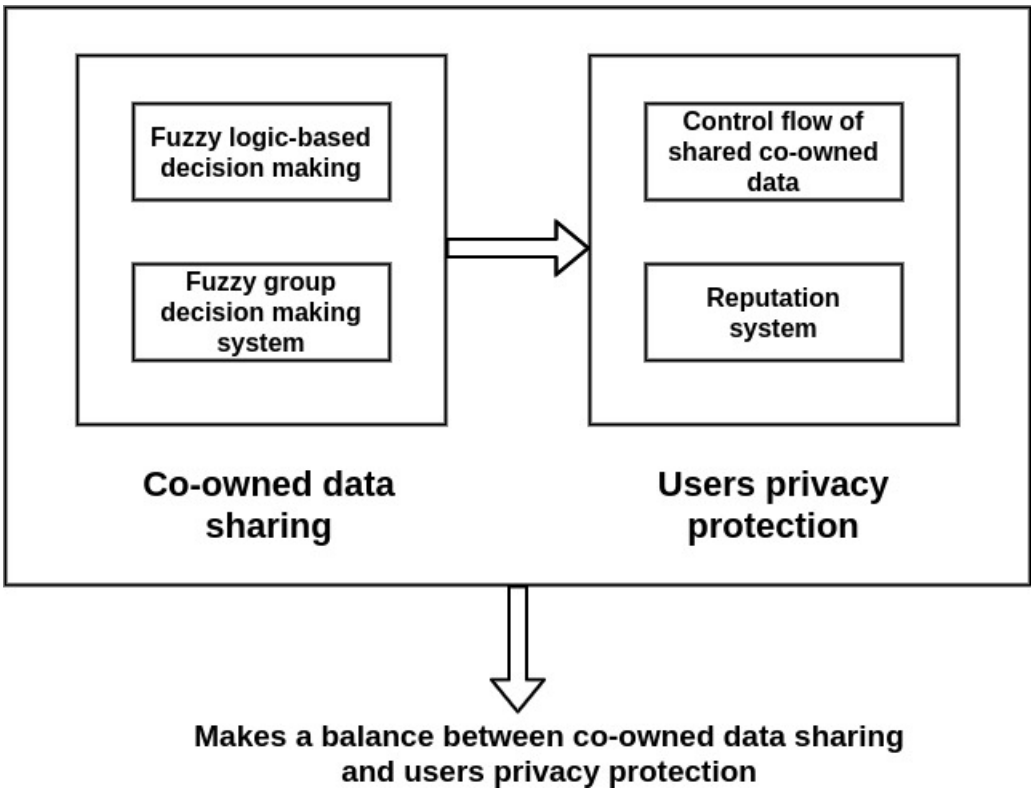

Figure 3.4: The whole picture of the developed framework

Chapter 4

Fuzzy Logic-Based Decision Making in Co-owned Data Sharing Processes in OSNs

In Chapter 2, existing decision expression has been introduced in current online social networks which only contains the Boolean Decision expressions. However, people neither use Boolean decision expressions in their daily lives actions' nor they share the information with others. Despite, such decision expressions have not been included in any existing social network platforms. This chapter presents a fuzzy logic-based decision making structure and models where the data sensitivity and the confidence in the targeted group or person are used to make the fuzzy decision. The reason for using fuzzy logic-based decision making system is that decision expressions are restricted into the Boolean decision expressions which means they are not close to the real life decision expressions although OSNs are considered reflecting people' daily lives.

4.1 Fuzzy Logic

Fuzzy logic was introduced by Zadeh Zadeh (2008), he explained the main difference between classical logic (*i.e. Boolean logic*) and fuzzy logic. Based on the definition, the main difference between fuzzy logic and classical logic is that the classical logic deals with true or false while fuzzy logic assigns true or false to a degree. Fuzzy logic helps common sense reasoning with uncertainty and vague propositions dealing with natural language and serves as a basis for decision analysis. Fuzzy logic aims to provide a basis for approximate reasoning with uncertainty propositions and it reflects rightness and vagueness of natural language in common sense reasoning. The main difference between fuzzy logic and Boolean logic is that fuzzy logic is based on possibility theory, while Boolean logic is based on probability theory Smets and Magrez (1987). Another difference between fuzzy logic and Boolean logic is that Boolean logic is a class of those sets having sharp boundaries while fuzzy is a class of those sets having un-sharp boundaries. In Boolean logic, there is no uncertainty about the boundary's location of a set while in fuzzy logic, there always exists uncertainty about the boundary's location of a set.

In real life, decision making is a challenging process because of incomplete and imprecise information in situations in decision making process. These incompleteness and vagueness factors point the importance of fuzzy environment Ishizaka (2014). In a decision making process, people use their knowledge or their subjectivity to make a decision in their daily lives. However, fuzzy logic was introduced to use the combination of subjective and objective knowledge, therefore, both equations and linguistic terms should be used in a decision making process.

With the development of Web 2.0 technologies, the usage of OSNs have also increased. And people have started posting their daily lives activities in OSNs platforms and OSNs

posts have started reflecting those platforms' users lives. However OSNs platforms expressions have always been limited and they have never reflected real life expressions McGoldrick (2013). OSNs users have also faced difficulties when they take decisions in a data sharing process in OSNs Wang et al. (2011). Based on fuzzy logic definition, fuzzy logic has proved itself for dealing with uncertainty situations. With this respect, we use fuzzy logic in co-owned data sharing processes in OSNs platforms with an extension on decision expressions. In classical logic, decision expressions are *yes* and *no*, however, fuzzy logic adds *maybe* expression in to the decision expressions sets.

4.1.1 The fuzzy set concept

A membership function was established by Zadeh (2008) when fuzzy logic was introduced because membership function was the main difference between fuzzy logic and classical logic. In fuzzy sets, a set is defined and an element then can be indicated either beings belonged to the set or not being belonged but with its degree. For example, it is a very subjective view to classify a person into classes such as young, mature, adult, and old although there is no certain threshold to place a person into those classes. In fuzzy logic, a continues process is defined in which the membership of a person to each set goes from 0 to 1.

Let S be a classical unlimited or limited set. A real function $\mu \implies$ [0,1] is defined the membership function of A and defines the fuzzy set A of S. This is the set of all pairs (s, μ_A(s)) with s $\in$ S.

Memberships functions are the determination features for a fuzzy set. In order to specify the main difference between see the following table. Let us assume that X=$\{x_1, x_2, x_3\}$. The classical subsets and the fuzzy sets of X can be defined as in Table 4.1. In the classical

logic set, the maximum value of each x_i element is taken to compute the union of A and B. The same way can be taken in fuzzy intersection value of two sets, however, the minimum of the membership values can be used to compute. In fuzzy sets, the maximum or minimum of the membership values are defined as one alternative pair of definitions of the union or intersection operations. There are various membership functions in fuzzy sets.

Figure 4.1 shows the geometrical representation of the fuzzy sets membership functions. The role of the membership functions has a vital importance in the performance of fuzzy representation. Each membership function has small different points in their calculation, for example, the Fuzzy Gaussian function transforms the original values into a normal distribution. The midpoint of the normal distribution defines the ideal definition for the set with the remaining input values decreasing in membership as they move away from the midpoint in both the positive and negative directions. The input values decrease in membership from the midpoint until they reach a point where the values move too far from the ideal definition and are definitely not in the set and are therefore assigned zeros. Another example is The Fuzzy Linear transformation function applies a linear function between the user-specified minimum and maximum values. Anything below the minimum will be assigned 0 (definitely not a member) and anything above the maximum 1 (definitely a member). It is entirely up to researchers to decide which membership function should be used in a fuzzy system based on the problem and distribution of data. In this thesis, the trapezoidal membership function is used.

Table 4.1: Difference between classical and fuzzy sets

Classical Sets	Fuzzy Sets
$X=\{x_1, x_2, x_3\}$	$X=\{x_1, x_2, x_3\}$
$A=\{x_1, x_2\}$	$C=\{x_1, x_2, x_3\}$
$A=1/x_1+1/x_2+0/x_3$	$C=0.5/x_1+0.6/x_2+0.3/x_3$
$B=\{x_2, x_3\}$	$D=\{x_1, x_2, x_3\}$
$B=0/x_1+1/x_2+1/x_3$	$D=0.7/x_1+0.2/x_2+0.8/x_3$
$A\cup B=1/x_1+1/x_2+1/x_3$	$C\cup D=0.7/x_1+0.6/x_2+0.8/x_3$
	$C\cap D=0.5/x_1+0.2/x_2+0.3/x_3$

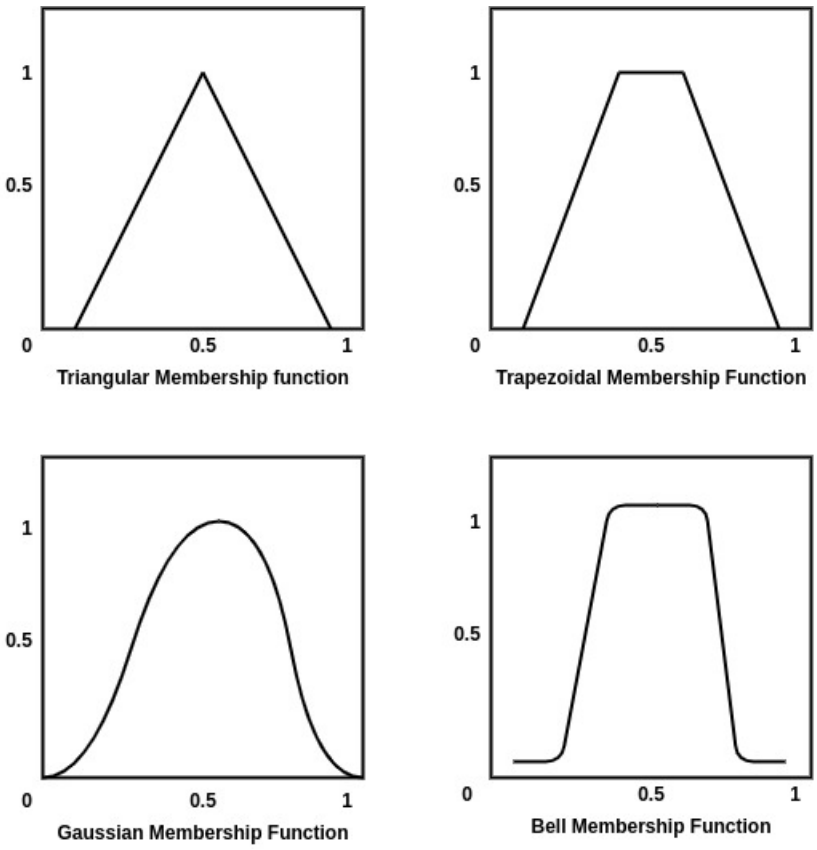

Figure 4.1: Geometric visualisation of fuzzy sets (Coupland and John (2007))

4.2 Co-owned Data Sharing Process

Decision making is an act of making selection between two ore more options Majumder (2015). In the real life, people do not make decision not only with the Boolean expressions but also with the fuzzy expressions Zadeh (2008). Actually, the issues and human approaches are not bivalent Tong and Bonissone (1980). Decision making is an important and challenging process, due to the fact that decision makers face difficulties like uncertainty and doubts while making decisions. The reason being the subjectivity in the natural language. Therefore, researchers have focused on developing more accurate mathematical and specialist decision making systems such as expert systems, neural networks, fuzzy logic, and machine learning Das (2016); Yadav et al. (2018); Sanayei et al. (2010); Yager (2018).

In this chapter, the fuzzy logic-based decision making is used to make a decision on co-owned data with the data sensitivity and the confidence in targeted group. The input variables for the fuzzy system are the data sensitivity and the confidence value. Therefore, it is important to give more details about the fuzzy system inputs.

Data Sensitivity: The sensitivity of the information or data and the confidence in the targeted group or person, who will have access to the shared content, are crucial criteria to make a decision.

4.2.1 Criteria to make a decision in co-owned data sharing processes

According to criteria provided by The General Data Protection Regulations (GDPR) Commission (2019), it is necessary to clarify that whom the content will be shared with and whether the content discloses someone's id. Based on the GDPR rules which are defined

in the above regulation, we can deduce that people need to know the sensitivity of the content and confidence level they have in the targeted group or individuals to decide whether to share the content or not. As a result of deduction, two general factors can be used as inputs for making a decision which are data sensitivity and confidence value in targeted group. The data sensitivity value is computed by using the number of unauthorised users Xu et al. (2019); Rathore and Tripathy (2017), which shows that the number of people whom the owner has relationship (*i.e. friendship*), is an important factor in data sharing process. As a result, having relationship with targeted group of data is important since OSNs' users usually share their contents with the people who they have connection with.

4.2.2 Effective features on the data sensitivity and the confidence in targeted group

In general, users are asked directly to set the data sensitivity value Petkos et al. (2015) in order to define the level of data privacy. However, users may not have enough knowledge to set the data sensitivity value. It might be easier to ask their choices on the data security features which helps in the calculation of data sensitivity values. To do so, we provide a model in which CIAPP data security features are used to calculate data sensitivity value. Users choose the features that make them worried about their data. The model decreases the difficulty for users when the data sensitivity is set because users only need to choose the features instead of defining the data sensitivity score.

Details of the CIAPP data security features are as follows; Confidentiality is the protection of personal information and it means keeping a user's information between the user and an OSN platform, and not releasing other users. Data integrity is the maintenance assurance of the accuracy and consistency of data over its entire life-cycle, and is a critical aspect

to the design, implementation and usage of an OSN platform which stores, processes, or retrieves data. Data availability is the process of ensuring that data is available to users, when and where they need it. Data privacy is the right of a user to have control over how data is collected and used. This is because protecting user data and sensitive information is a first step to keeping user data private. Data possession assures that the control of data is under control of the owner in OSNs.

Table 4.2 indicates the related features to data sensitivity in OSNs. Table 4.2's features are deduced from Cherdantseva and Hilton (2012), the data security features are divided into five circles based on the thesis goals and disciplines. Deduced five features are combined to measure the data sensitivity (S_d) in OSNs. As it is seen on the table, the chosen features are related to information security discipline.

Table 4.2: Related Information Security Features to OSNs

Subject of Protection	Discipline
Confidentiality	Information
Integrity	Information
Availability	Information
Privacy	Information
Possession	Information and Network

4.3 Model Development for the Data Sensitivity Value and the Confidence Value in Targeted Group

After specifying the effective features on the data sensitivity value and the confidence value in targeted group, we have developed models for the data sensitivity and for the confidence value in targeted group. This section gives the mathematical models of the

data sensitivity value and the confidence value, which are used for input values in fuzzy-logic decision making system in this thesis.

4.3.1 Data Sensitivity Model and Its Related Features

Information security is one of the fundamental concerns in the organisations and online social platforms as the accessibility of information becomes much easier with the Web 2.0 platforms. In order to ensure the protection of the data security; Confidentiality, Integrity, and Availability (CIA) model was developed with the intention to guide policies to ensure the data security Samonas and Coss (2014). In the CIA model, confidentiality is a boundary to limit access to data, whereas integrity is a guarantee of limited access to the data, and availability is ensuring that the data is only accessed by authorised people Akkuzu et al. (2018); Cherdantseva and Hilton (2013); Sattarova Feruza and Kim (2007).In order to protect users' sensitive data, the information security is also needed in OSNs Hu et al. (2011). The data sensitivity is a measurement which is calculated with the number of unauthorised people, however, Akkuzu et al. propose a new model in which Privacy and Possession features are added to extend the CIA model Akkuzu et al. (2019c). So, the privacy and possession features have been added to the CIA model. Hence, privacy and possession features are used to control data security in OSNs platforms. Privacy feature is the right to have some control over how a person's information is collected and used, and possession is the quality of ownership or control.

In this thesis, the data sensitivity value shows co-owners' concerns about their information being disclosed by owner's co-owned data sharing. Co-owners' concerns are calculated with the probability of their choices on CIAPP features. Equation 4.1 shows the developed model for co-owned data sensitivity calculation in OSNs. In the model, S_d represents

the data sensitivity, it ranges from 0 to 1. The numerator gives the summation of the CIAPP security features probabilities, in which P_i indicates the probability of each CIAPP feature concerns that is selected by co-owners and w_i is the weight of the properties. The denominator indicates the total number of data security features. In this thesis, f_j is equal to 5 because the number of data security features used in this work.

$$S_d = \frac{\sum_{i=1}^{m}(P_i * w_i)}{\sum_{j=1}^{m}(f_j)} \tag{4.1}$$

Algorithm 1 is the representation of the data sensitivity value calculation. In the algorithm, first *for* loop is for the number of decision makers. It runs until all decision makers make choices on the data security features. The second *for* loop is for choosing the data security features. When a feature is chosen, the probability of the chosen feature is calculated with its weight value. Once all decision makers make choices on the co-owned data security features, the summation is calculated. In the last step, the data sensitivity value is obtained with the summation of the probabilities of features and the number of features.

Figure 4.2 presents the changes on the data sensitivity (*Sd* model) with the probabilities of the data security features (*confidentiality, integrity, availability, privacy, and possession*). As it is aforementioned, the data sensitivity value ranges [0,1]. Figure 4.2 shows that the developed model S_d (see *Equation 4.1*) ranges in [0,1].

4.3.2 Confidence in the Data Targeted Group

Confidence is defined as a trust that one person has to believe the other person and this will not cause any harm to him Shin (2010). In people's social lives, confidence is one of the critical points to decide whether to share their information or not. It has been addressed

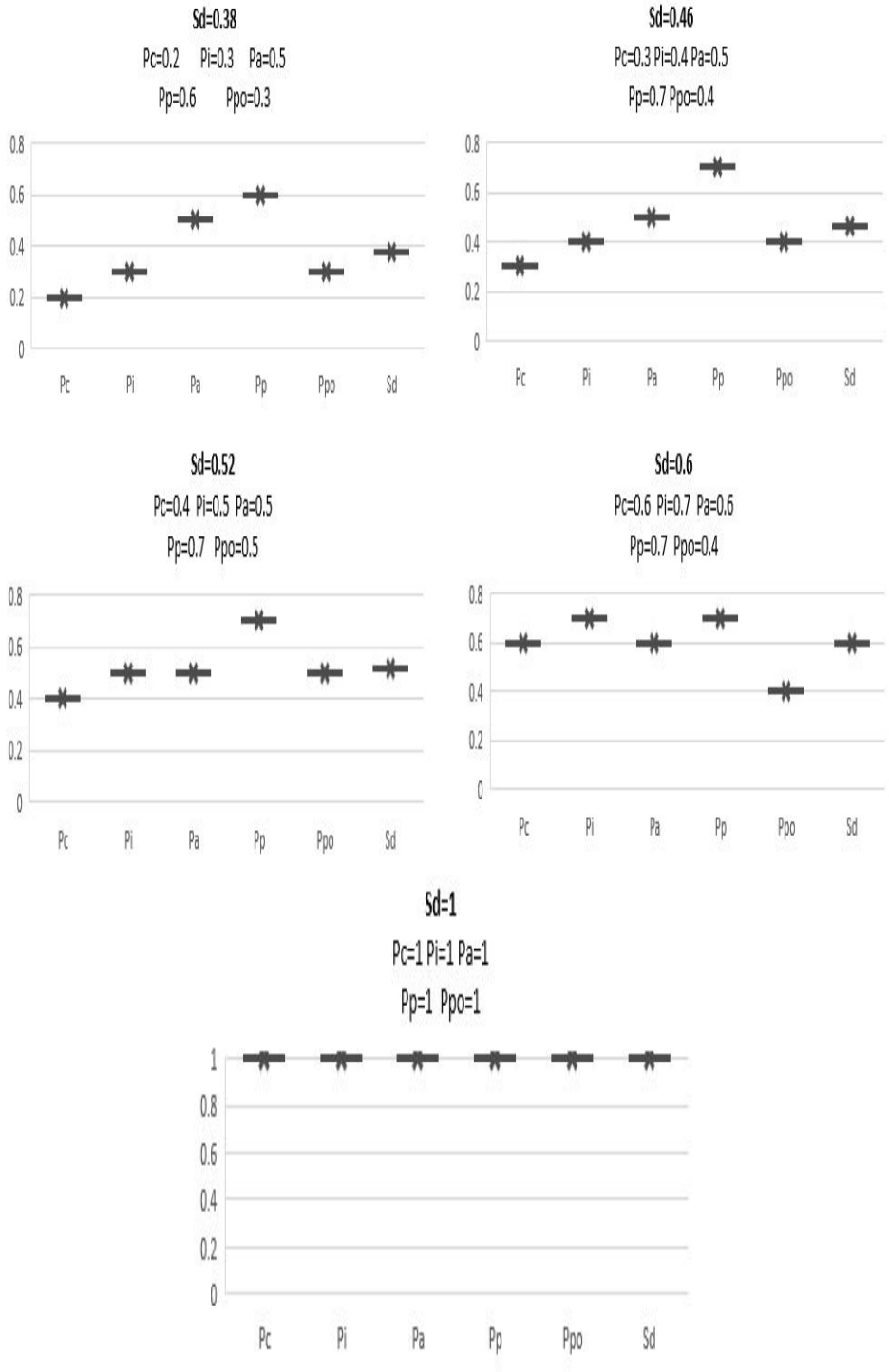

Figure 4.2: S_d Model Changes with the Probabilities Values of Data Security Features

input : The number of decision makers (co-owners) m and the number of data security features n
output: Data Sensitivity ValueS_d

for $k \leftarrow 1$ **to** m **do**
    the number of decision makers;
    for $l \leftarrow 1$ **to** 5 **do**
        $w_i = 1$**: the weights of the CIAPP features**
        Confidentiality$\leftarrow Pc[Pc, w_i]$;
        Integrity$\leftarrow Pi[Pi, w_i]$;
        Availability$\leftarrow Pa[Pa, w_i]$;
        Possession$\leftarrow Pp_o[Pp_o, w_i]$;
        Privacy$\leftarrow Pp[Pp, w_i]$;
    end
    Sum=Pc+Pi+Pa+Pp+Pp_o
    S_d=Sum/5
end

Algorithm 1: Algorithm for Calculating Co-owned Data Sensitivity Value

that the trust is also important in OSNs to share the data with other users Shin (2010); Dwyer et al. (2007b).

The Equation 4.2 indicates the relation value between the owner and people who are in the targeted group for the co-owned data. In the model, R_{o-u} is the representation of the relationship numerical value which exist between the owner and each user who is in the targeted group for the co-owned data. If the owner and a user has relationship, then the relation value is assigned to 1. n indicates the size of the group, it shows the number of people in the targeted group. τ represents the trust values that appears between owner and the users in the targeted group.

$$R_{o-u} : f(r_{o-u1}, r_{o-u2}, ..., r_{o-un}) = \frac{\sum_{j=1}^{n}(r_{oj}) * \tau_{o-uj}}{n} \tag{4.2}$$

The model below indicates the relation between co-owners (i.e. stakeholders) and the members of the data targeted group. In the model, $f(r_{co1-u1}, ..., r_{co1-uj}, ..., r_{con-uj})$

is the function which takes the relationship values between each co-owner and user in targeted group. τ_{co-uj} is the illustration of the trust value between each co-owner and each user in the targeted group.

$$R_{coi-u} : f(r_{co1-u1}, ..., r_{co1-uj}, ..., r_{con-uj}) = \frac{\sum_{j=1}^{n} (r_{coj-uj}) * \tau_{co-uj}}{n} \tag{4.3}$$

Model 4.4 is the combination of the model 4.2 and model 4.3. The model gives the final relation value for the fuzzy-logic decision system's fuzzification.

$$R = R_o * \prod_{l=1}^{c} R_{ci} \tag{4.4}$$

C_f is defined as a trust value to believe someone Kim and Ahmad (2013). The connection between trust and sharing private information or sensitive data is defined as confidence value. Therefore, the data sensitivity value and the relation value are important to develop confidence model. Model 4.5 indicates the confidence value in targeted group, it ranges between 0 and 1.

$$C_f = 1 - S_d * (1 - R) \tag{4.5}$$

Figure 4.3 presents the changes on the model 4.5 with the model 4.1 and 4.4. The results show that the value of the confidence does not exceed 1, we keep the data sensitivity value stable with changes on the relation value. The important point of given figures is that the confidence value increases when the data sensitivity value is low. For instance, the fluctuation on the confidence value when the sensitivity value is *0.01* presents that the confidence value is either 1 or has a value, which is close to *1*, regardless of the relation value. When the sensitivity value goes up and the relation value goes down, the confidence value decreases.

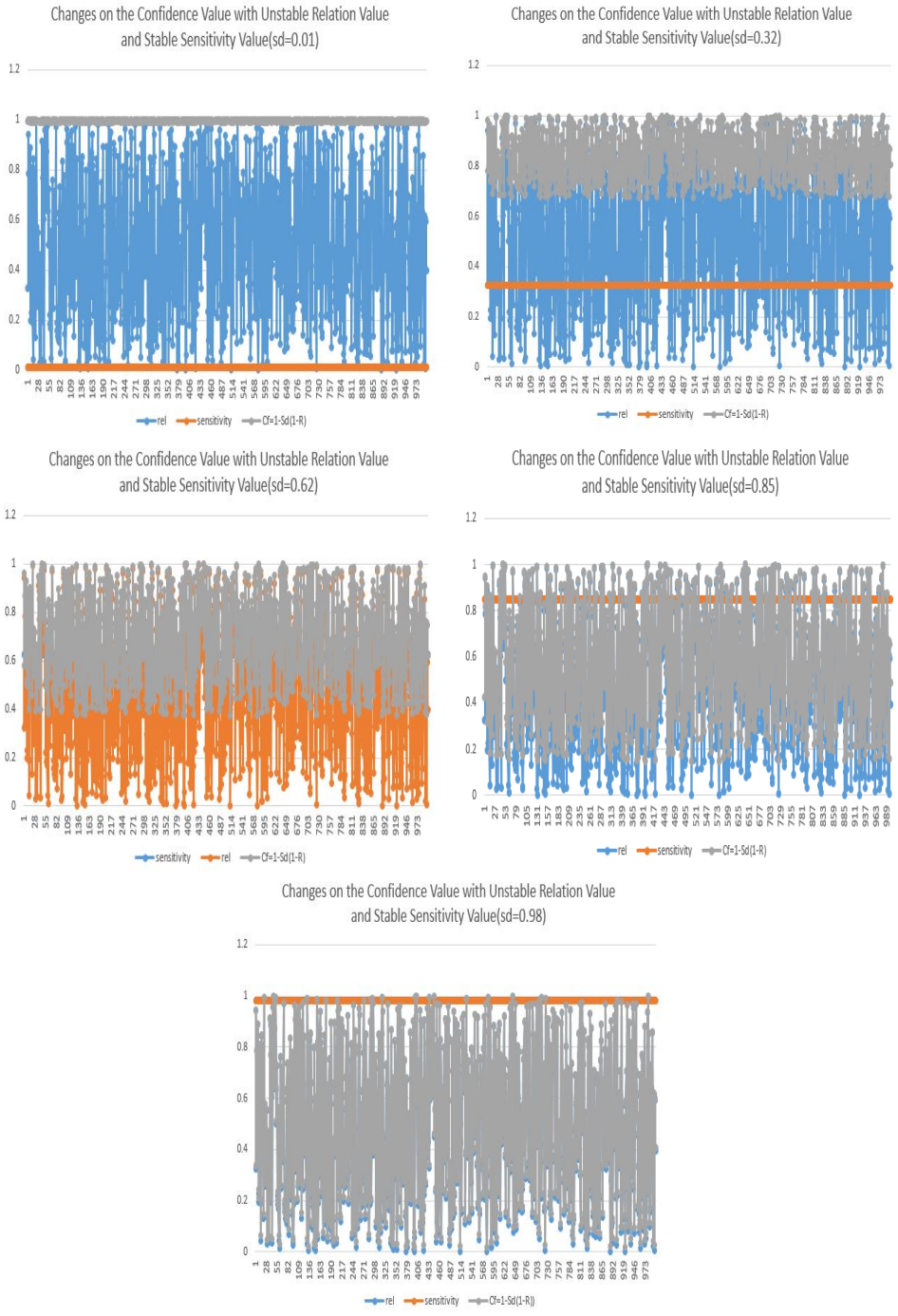

Figure 4.3: Fluctuation on the Confidence Value with the Data Sensitivity Value and the Relation Value

Fuzzy Decision with the Data Sensitivity and Confidence Value

A fuzzy logic decision making system consists of three main components, which are *Fuzzifier, Fuzzy Inference Engine*, and *Defuzzifier*. Figure 4.4 presents this thesis fuzzy system with input variables and output variables. In fuzzification process, crisp values are taken as input values and fuzzy input sets are given as output values. It is basically the process of associating input values with the linguistic variables. In intelligence process, the fuzzy input sets which are produced in the fuzzification stage, and the fuzzy rules are taken as input values and fuzzy set output values are given as output. In defuzzification stage, the fuzzy output sets are taken as input values and crisp output values are given as output values of the defuzzification stage. The main purpose of the defuzzification is to convert an imprecise value into a precise value.

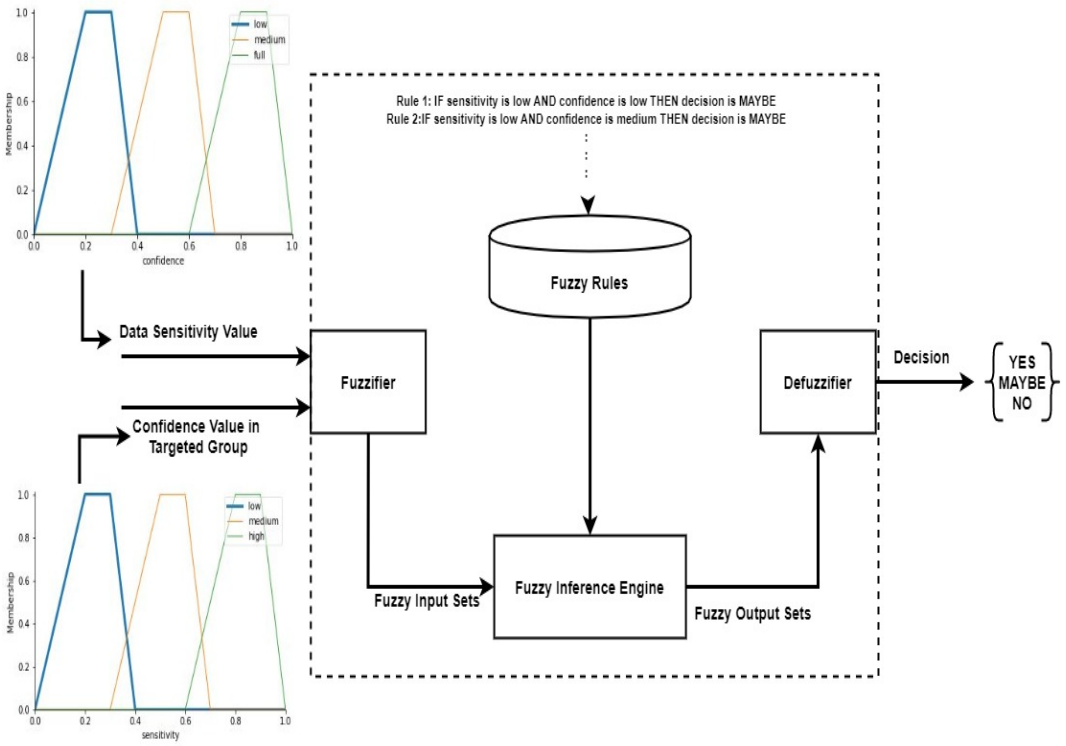

Figure 4.4: Fuzzy Logic Decision Making System Structure

We use trapezoidal membership functions in order to generate membership functions. In addition, we use C-Means Clustering algorithm to generate clusters and to construct membership functions.

- Input variables' values and output variable values are formed into three clusters. These three clusters' centers are used as the centers of triangular fuzzy membership functions.
- The maximum and minimum values of each cluster are used as two vertexes values for each of triangular membership functions.
- The maximum and minimum values for triangular membership functions are formed by increasing and decreasing 'b' vertex values.
- Trapezoidal membership functions variables values are calculated by increasing the minimum vertex value of triangular membership function and decreasing the maximum vertex value of triangular membership function .

Table 4.3 represents the input variable, input variables' values' ranges, output variable, and output variable values. All the values of inputs variables' and output variable values range in [0,1].

Figure 4.5 shows the membership function values for the data sensitivity value, the confidence value, and the decision value with their linguistic terms. As we have shown in Figure 4.4, we have input variables *Sensitivity Value* and *Confidence Value* and one output variable is *Decision*. Figure 4.5 shows the input variables and output variable ranges for membership functions and linguistic value for each range. Both input variables have three linguistic values *low, medium*, and *high* respectively. The output *Decision* has three values *no, maybe*, and *yes*.

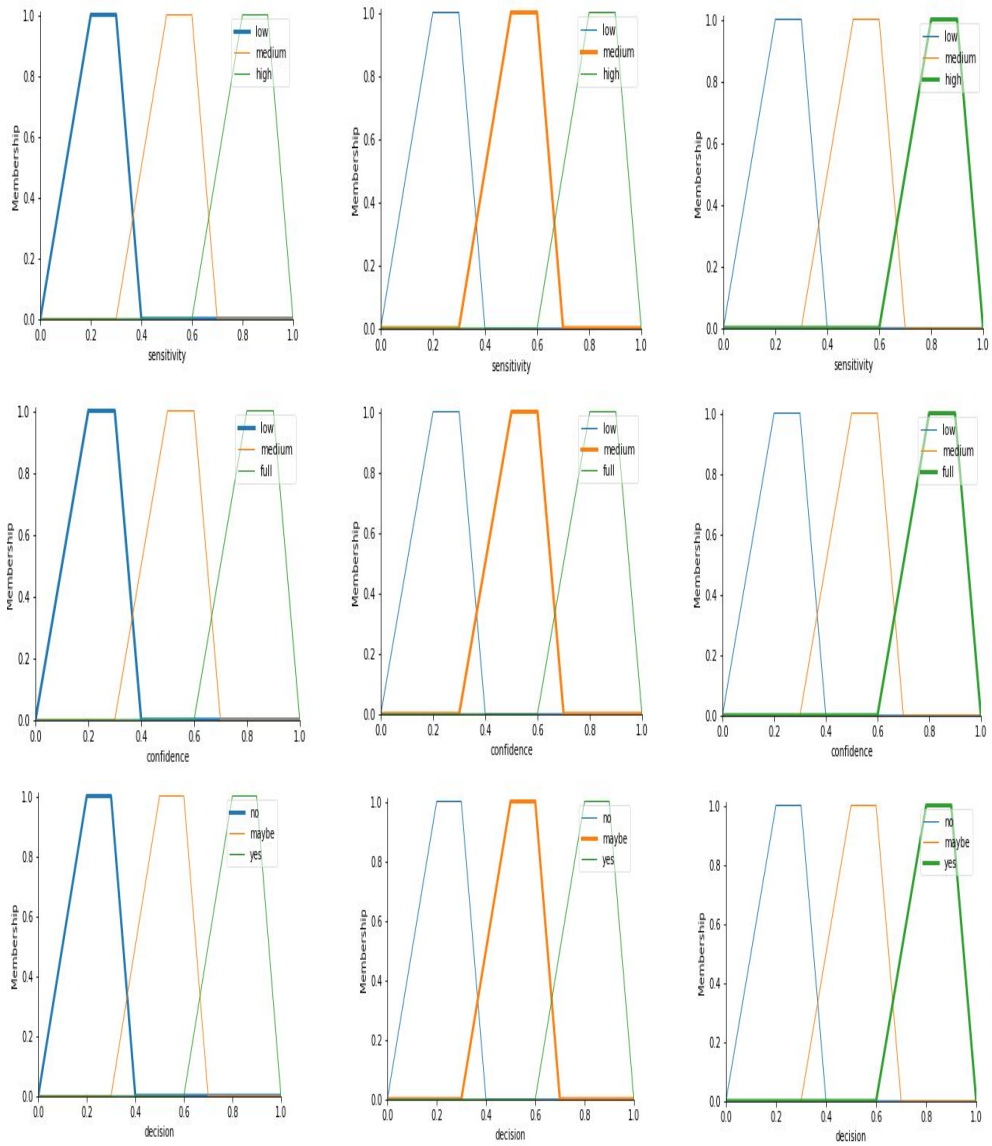

Figure 4.5: Membership Values for Each Input Values and Output Values

Table 4.3: Fuzzy System Decision Making Database

Linguistic Variables	Type	Membership Functions	Range
Sensitivity Value	Input	Low	Range [0,1]
Sensitivity Value	Input	Medium	Range [0,1]
Sensitivity Value	Input	High	Range [0,1]
Confidence Value	Input	Full	Ranges [0,1]
Confidence Value	Input	Medium	Ranges [0,1]
Confidence Value	Input	Low	Ranges [0,1]
Decision	Output	Yes	Ranges[0,1]
Decision	Output	Maybe	Ranges[0,1]
Decision	Output	No	Ranges[0,1]

The focus here is on nine fuzzy rules for its fuzzy system, the rules are given in Table 4.4. The *AND* operator is used for the fuzzy rules. The *AND* operator considers the minimum value among membership functions. We have used the *Fuzzy-C Means* algorithm to generate the membership function values for input and output variables values (see Section A.1 in Chapter A)

Table 4.4: Fuzzy System Decision Making Rules

Rule No	Fuzzy Rules
rule1	sensitivity['low'] ⋀confidence['low'], decision['maybe']
rule2	sensitivity['low'] ⋀confidence['medium'], decision['maybe']
rule3	sensitivity['low'] ⋀ confidence['full'], decision['yes']
rule4	sensitivity['medium'] ⋀ confidence['low'], decision['maybe']
rule5	sensitivity['medium'] ⋀ confidence['full'], decision['yes']
rule6	sensitivity['medium'] ⋀ confidence['medium'], decision['maybe']
rule7	sensitivity['high'] ⋀ confidence['low'], decision['no']
rule8	sensitivity['high'] ⋀ confidence['medium'], decision['maybe']
rule9	sensitivity['high'] ⋀ confidence['full'], decision['yes']

4.3.3 Experimental Study of the Fuzzy Rules

In a fuzzy logic decision making system, the defuzzification is the process of producing a quantifiable result in Crisp logic, given fuzzy sets and corresponding membership degrees.

Defuzzification maps a fuzzy set to a crisp set Van Leekwijck and Kerre (1999). In Table 4.4, given nine rules are transformed into a fuzzy result in which the result is described in terms of membership in fuzzy sets. Figure 4.6 presents the outcome of the fuzzy system with different data sensitivity value and confidence value.

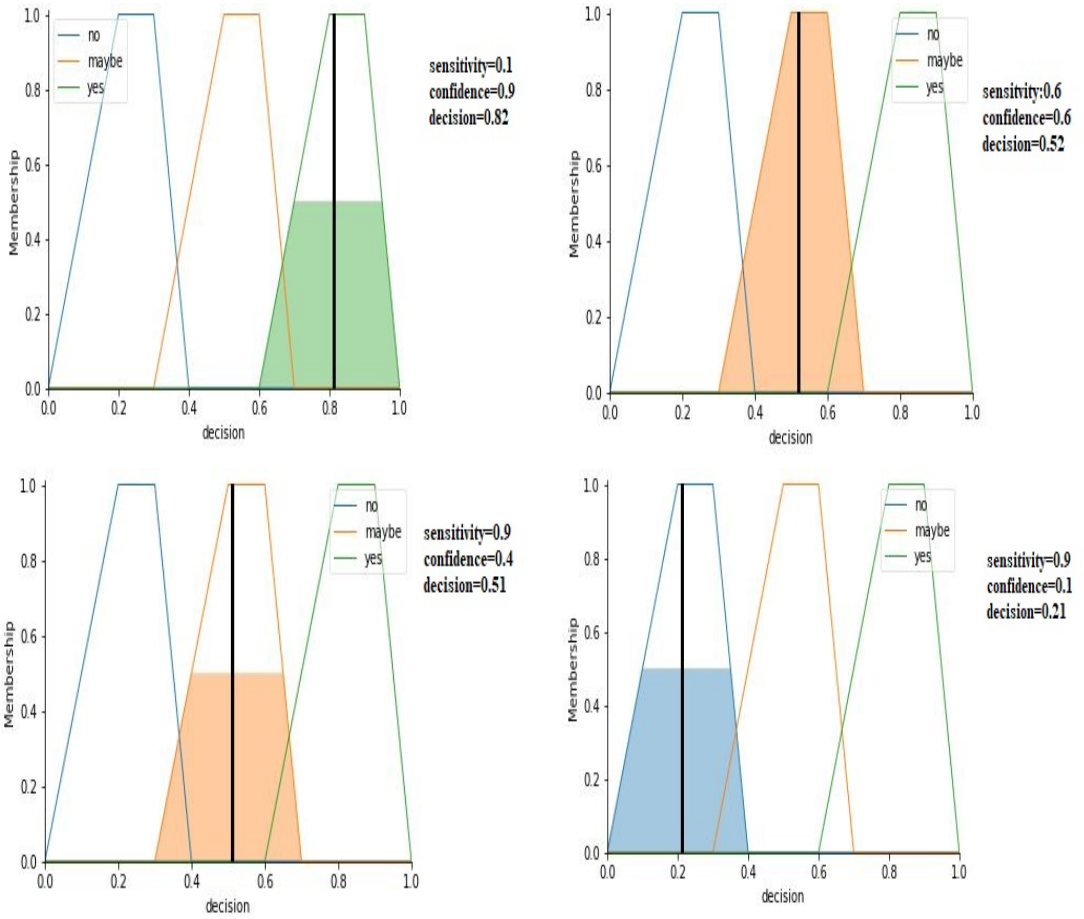

Figure 4.6: Output Values of Defuzzification

4.4 Conclusion

Making decision on data sharing processes has been a crucial issue, especially when multiple people are involved into the content of data. Every person has their own decision

for a co-owned sharing process since each of them has their own concerns on the sharing process. The most challenging part of decision making on those type of data is to make a decision as closest as to the the real world decisions' expressions. To do so, fuzzy logic-based decision expressions are needed on data sharing processes in OSNs.

Although, some of shared data in OSNs are associated with multiple users, the data sensitivity value is decided by a single user in the previous works. However, the data may not be sensitive to the owner while it is highly sensitive to the other users. This Chapter covers the gap in the development of data sensitivity S_d model, the developed model takes all users' concerns on the data security features. Related security features are chosen with the relevance of information security and network security, therefore, the data sensitivity model in this thesis is a unique and novel model.

In this chapter, We have used a fuzzy logic-based decision making system, in which the data sensitivity and the confidence value in the targeted group are used as input variables and a fuzzy logic decision is the output variable. The used fuzzy system's variables' (*confidence* and *data sensitivity*) models have been developed by the researcher. The data sensitivity value should not be a single-handed value for co-owned data in OSNs; therefore, the developed data sensitivity value has not been decided by the data owner. Co-owners' opinions are important for the data sensitivity since the content of data is not only related to the data owner but also related to co-owners. In order to calculate the data sensitivity value, the data security features have been used with consideration of features that are related to information security and network security.

The used models can be used in other areas, where the content of data is considered to be related to multiple people. Because the data sensitivity value is not only related to OSNs' data, but any content of data could be sensitive. The used fuzzy system has already been used in forensic data sharing process Scheidt et al. (2020). Furthermore, this decision

making system can make decisions closer to real life decision expressions and can also help in arriving at more appropriate decisions.

Chapter 5

Fuzzy Consensus Reached Group Decision Making

This chapter describes the consensus-reached group decision making in details and also provides the trust values τ usage in Extended Induced Ordered Average Weighted (EIOWA) model which can be used to weight the co-owners' opinions. The main aim of this chapter is to adapt the EIOWA technique for obtaining a consensus-reached group decision.

In the previous chapter, we have introduced the fuzzy logic-based decision making for OSNs' platforms along with proposed model for calculating the data sensitivity value and the confidence value in the data targeted group. The developed fuzzy logic-based system takes a decision with data sensitivity and the confidence value just like the real life decisions. This chapter presents a consensus-reached group decision making approach for OSNs' co-owned data sharing processes. Taking a decision in co-owned data sharing processes should include involved users' opinions in the sharing process. Applying group decision making is the way to take every group member's opinions into consideration when

a decision is taken. Co-owned data relates to more than one user in OSNs platforms, therefore, GDM approaches are needed to be applied to decide whether data should be shared or not. In OSNs' co-owned data sharing processes, all users who are involved in a content of data should take a decision where none of the user have to worry about their privacy if the content is shared. The Consensus reaching step is the most important stage in GDM processes. The reason is that the consensus reaching process consists of discussion rounds and obtaining the best decision which is taken by the group members. With respect to the group decision making approaches' requirements, this chapter introduces a consensus-reached group decision making model with EIOWA technique.

5.1 From the OWA Technique to the EIOWA Technique

Prior to our approach, we first explain the group decision making methods from the ordered weighted averaging (OWA) to EIOWA method. This is because of the fact that EIOWA technique is used as ground work for our approach.

The OWA operator introduced by Yager (1988) is an aggregated operator of the maximum and minimum average criteria. In the OWA operator, the input data is reorganised in descending order and the weights of the input data are used for the weights of the ordered positions of the input data instead of being the weight of the input data Zeng and Su (2011). The aim of the OWA operator is to aggregate the criteria functions in decision

making systems. An OWA operator is defined as follows;

$$\begin{aligned} OWA(a_1,...,a_n) &= \sum_{j=1}^{n} w_j b_j \\ &where, \\ \mathbb{R}^n &\mapsto \mathbb{R} \\ w_j &\in [0,1] \\ \sum_{j=1}^{n} w_j &= 1 \end{aligned} \tag{5.1}$$

In the equation, b_j is the jth largest of the a_i. In the OWA method, an argument a_i is not weighted with a particular w_i but a weight value w_i is placed to a particular ordered position i of the arguments. Yager and Filev (1999) introduced induced ordered weighted averaging (IOWA) method which is considered to be an improved type of OWA technique. In the IOWA method, one pair is used to induce an ordering over the second pair and is then aggregated Qian and Xu (2006). The difficult point of IOWA is to have the argument with the numerical values because linguistic variables are more preferable in the applications Xu (2005).

$$\begin{aligned} IOWA(< u_1,a_1 >,...,< u_n,a_n >) &= \sum_{j=1}^{n} w_j b_j \\ &where, \\ (\mathbb{R}x\mathbb{R})^n &\mapsto \mathbb{R} \\ w = (w_1,w_2,...,w_n)^T & \\ w_j &\in [0,1] \\ \sum_{j=1}^{n} w_j &= 1 \end{aligned} \tag{5.2}$$

b_j is the a_i value in $< u_i, a_i >$, u_i is the order inducing variable and a_i is the argument variable. In the IOWA operator, the numerical values were used for the aggregation. Due to the linguistic arguments deficiency in IOWA method, Xu (2006) introduced EIOWA method which was used to aggregate linguistic arguments in a group decision making process. An EIOWA operator is defined as follows;

$$\begin{aligned} EIOWA(< u_1, s_{a_1} >, ..., < u_n, s_{a_n} >) &= w_1 s_{\gamma_1} \oplus ..... \oplus w_n s_{\gamma_n} \\ &= s_{\bar{\gamma}} \\ &where, \\ w = (w_1, w_2, ..., w_n)^T & \\ w_j \in [0,1] & \\ \sum_{j=1}^{n} w_j = 1 & \\ \bar{\gamma} = \sum_{j=1}^{n} w_j \gamma_j & \end{aligned} \tag{5.3}$$

s_{γ_j} indicates the s_{a_i} in $< u_i, s_{a_i} >$ having the jth largest u_i value, and u_i represents the order inducing variable. The important difference in the EIOWA model is to use s_i value, which is the linguistic variable. The progress of the EIOWA group decision making method from its starting point OWA method is as above. The main advantage of EIOWA method is that it uses the linguistic variables for arguments in decision making processes. According to Wei (2019), decision makers prefer to give their choices with linguistic variables rather then numerical values. With this respect, the EIOWA technique is used to make the group decision in this thesis.

5.2 The Need for Fuzzy Group Decision Making in OSNs

Prior to our approach, the need of group decision making in OSNs platforms is highlighted. The consensus reaching approaches in OSNs along with their strengths and weaknesses have been analysed.

The first consensus approach in OSNs was proposed by Alonso et al. (2013) in order to improve concurrency among decision makers. The main advantage of the proposed approach is to introduce the effects of trust relations real-time communication on social networks decision making process.

Li et al. (2013) proposed the Deffuant-Weisbuch model, in which hard opinion dynamics and soft opinion dynamics were studied. Hard opinion dynamics focus on a trust function with trust existence between users, whereas, the soft opinion dynamic focus on formation of individual opinions with other member's influence.

Brunelli et al. (2014) has improved the soft consensus approach in order to address the consensus evaluation problem. The proposed method aimed to reach consensus with aggregation of the maximum number of users.

In Wu et al. (2015a), a new consensus-reached group decision making approach has appeared. The proposed approach has used users' relations existence as a trust value, and uses the τ for weighting users' opinions.

Prior literature has shown that consensus-reached decision making is a need for social network platforms. It also clarifies that weighting users' opinions has been a problem because the relation existence should not be only the factor for weighting. In order to solve the problem of weighting users' opinions in OSNs' group decision making, as well as ensuring that a co-owned data sharing process needs a consensus-reached group decision

making for securing the sharing process, the following section introduces a consensus-reached group decision making for OSNs.

5.3 A Fuzzy Consensus-reached Group Decision Making on Co-owned Data Sharing Processes

In this part of the thesis, we created consensus-reached group decision making structure for co-owned data sharing processes in OSNs by using EIOWA method, where users' trust values are used to weight users opinions. Figure 5.1 represents the group decision making part in the main framework (see Figure 3.2 in Chapter 2). members.

As noted in the previous chapter, the targeted group and the data sensitivity are important values to make decision, however, those two values are not enough to make a secure data sharing in OSNs. Co-owners should be able to express how their data will be shared which means that what permissions should be given to the targeted group. Therefore, a secure co-owned data sharing process contains; groups decision making where the set of alternatives needs to be related to access permissions on the content of data.

In a GDM process, decision makers give their individual opinions on a given alternative set and either a moderator (i.e. service provider or a user) takes the responsibility for the final decision. By taking into the consideration, the aim of the current thesis is to analyse how co-owners give their choices on a given alternative set while the owner is the moderator, who is responsible to take the final decision.

As it is seen in Figure 5.1, there are two different fuzzy systems in the framework which work in parallel. The first one is the fuzzy logic-based decision making system whereas

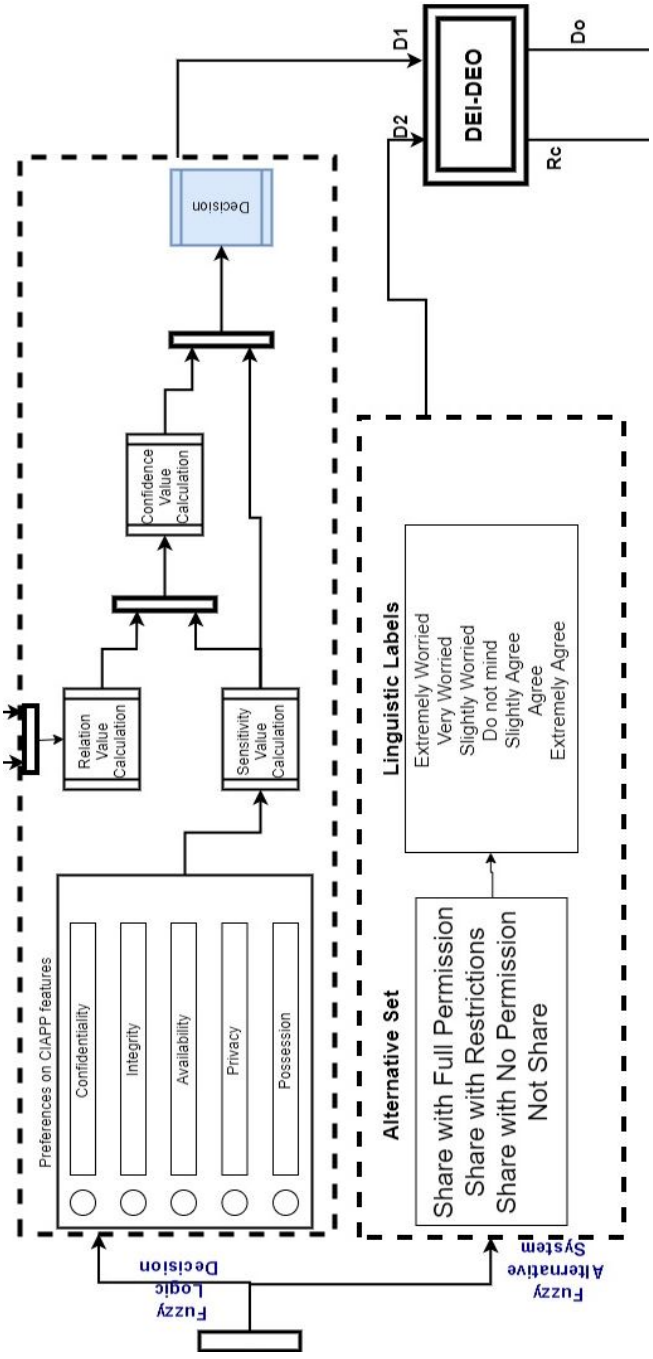

Figure 5.1: Consensus Group Decision Making Part of The Developed Framework

the other one is the fuzzy alternative system. In the fuzzy logic-based decision making system (Chapter 4), CIAPP features are used for data sensitivity and the fuzzy logic-based decision. The CIAPP features selection and the preferences on the given alternative set are provided by decision makers on the same time. The intention is to make sanity check between two decisions which means that fuzzy logic-based decision system's decision is consistent with the fuzzy alternative system's decision. For example, let us assume that the fuzzy logic-decision based system's decision is *NO* and the fuzzy alternative system's group decision is *Share with Full Permission*, the inconsistency between the two decisions can clearly be recognised. In order to eliminate such cases, the proposed framework checks decisions' consistencies with Decision In-Decision Out (*DEI-DEO*) part in the figure. The fuzzy logic-based system's decision (D_1) is fused with the fuzzy alternative system's output (D_2) in the DEI-DEO (Decision In-Decision Out) box. The framework has two outputs based on the output of the DEI-DEO. The system either gives recommendations to decision makers or notifies the owner with the best alternative.

Steps of the given part of the general framework are as follows;

- Notify DMs with the data, targeted group and the set of alternatives.
- DMs provide their choices on CIAPP features and provide their preferences on the alternatives.
- DMs' choices are used to compute the decision in the Fuzzy Decision System and the x_i is chosen with the *EIOWA* aggregation technique in Fuzzy Alternative System.
- The Fuzzy Decision System's output (*yes,maybe,or no*) is fused with the Alternative System's output(x_i).
- If the fused decision is meshed conveniently with each-other, then the x_i is recom-

mended to the data owner and the process is stopped.

Otherwise, a feedback mechanism is applied in which the owner can prepare some guidance and advice for decision makers to reach the consensus more easily.

- Finally, an advise is given to the decision makers and the first round is finished.

5.4 Fuzzy Alternative System for Consensus-reached Group Decision Making

The structural details of consensus group decision making model is given in Figure 5.2. The alternative set is the main part of any group decision making. An alternative set is given to the group members for giving them a chance to make choices on the given set. For co-owned data sharing in OSNs, options in the alternative set are as follows;

1. Share with full permission
2. Share with restrictions
3. Share with No permission
4. Not Share

The options in the alternative sets are general enough to cover all the situations in any co-owned data sharing processes. However, if the options need to be specified with more details, it does not create an issue with the proposed work. Decision makers (DMs) are people who are considered as co-owners in OSNs. It is expressed as; DM=i=1,2,...,n $\Leftrightarrow$ Co=i=1,2,...,n

As it is mentioned before, we use the EIOWA method, in which linguistic variables are used to make choices. However, it is important to highlight that the linguistic variables make the process easy for the group decision makers which is explained in the following section with its details.

In the Fuzzy Alternative System (see Figure 5.2), the group evaluates the given alternatives in order to make the most convenient decision for sharing co-owned data. The main advantage of the fuzzy alternative system is the elimination of the defuzzification step, an analytic formulation that can be easily implemented in software, and direct control of the shape of the input-to-output mapping surface. It is mostly used because of the ease of use in a system implementation. Decision makers may not be familiar with numerical values, however, they might use linguistic values in an easier way. The linguistic terms are provided in the fuzzy alternative system. The main criteria is that the group's decision needs to be a concurrent decision with the fuzzy logic-based decision system's output in which the group members' make their choices on the CIAPP features and the confidence in the targeted group is used. The set of alternatives with the linguistic variables are given to the co-owners.

5.4.1 EIOWA Method with Usage of Users' Trust Values

In GDM processes, weighting group decision makers' opinions is considered to be an important step. In OSNs, the major challenges are applying the group decision making and weighting decision makers' opinions. Wu et al. (2017) has addressed the weighting decision makers challenge in social networks. In addition to this, the difficulties of the trust usage in group decision making across social networks has also been discussed. This part of the thesis introduces not only the group decision making process

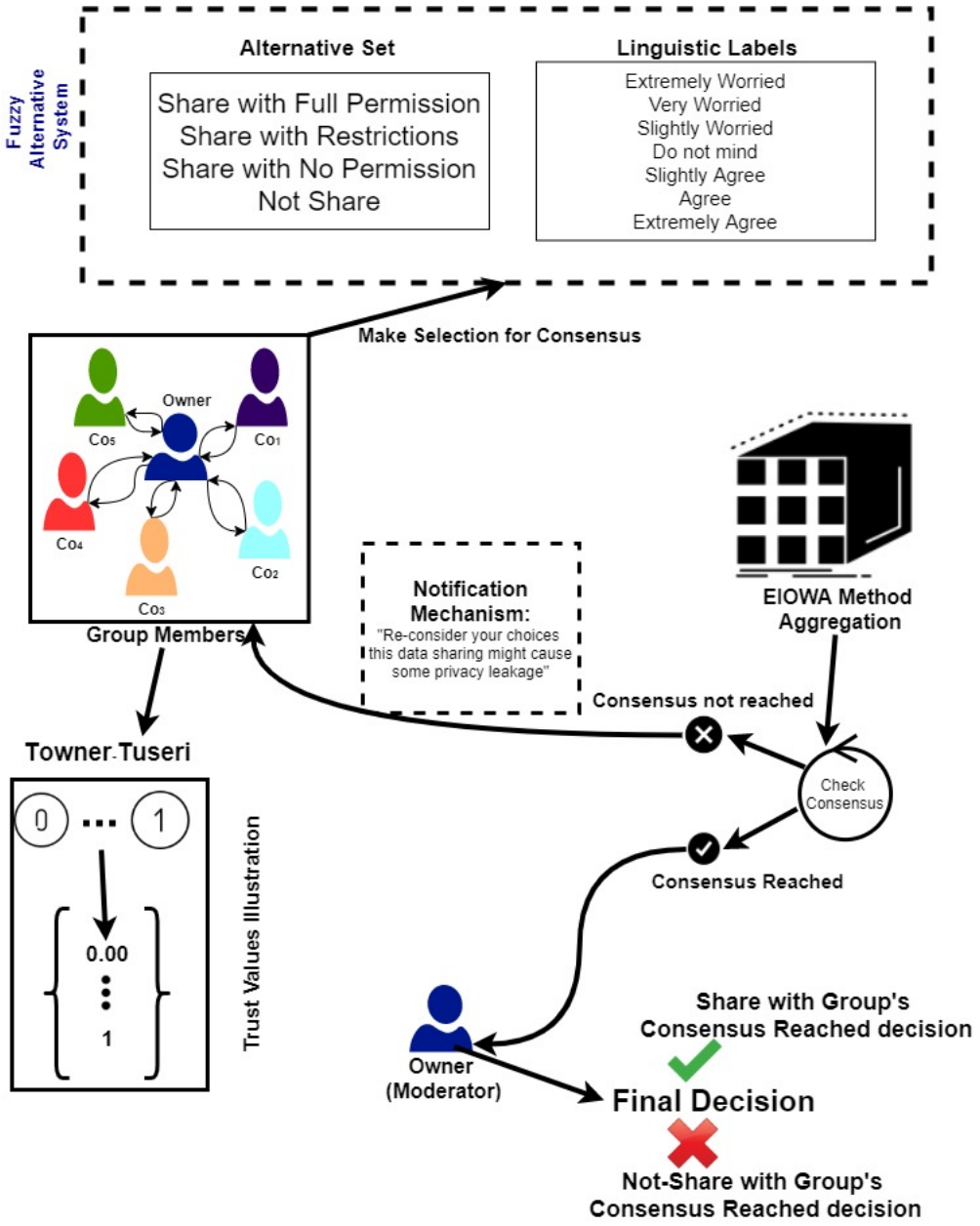

Figure 5.2: Trust values usage and EIOWA technique usage for consensus model in co-owned data sharing

but also makes use of users' trust values for weighting the decision makers' opinions. In Algorithm 2, the steps for implementing EIOWA technique with the use of trust values. The first step is utilising the EIOWA technique for the developed framework. Then collect the additive linguistic preference relation values into an aggregated linguistic preference relation. The third step is the aggregation of the alternatives with given operator. The last step is to rank the highest valued option among the aggregated values.
Result: Ranked alternative

1 **while** *While n > the number of co-owners* **do**

2 **Step 1:** Utilise the EIOWA operator

$\hat{r}_{ij} = EIOWAw(r_i^{(1)}_j, r_i^{(2)}_j, ..., r_i^{(l)}_j)$

3 *i,j*=1,2,3,4,...,n are associated to the trust values (τ) between the data owner and the co-owners (DMs).

$$EIOWA\tau(s_{\alpha 1}, s_{\alpha 2}, ..., s_{\alpha n}) = \tau_1 s_{\beta 1} \otimes \tau_2 s_{\beta 2} \otimes ... \otimes \tau_n s_{\beta n} = s_{\bar{\beta}} \tag{5.4}$$

where $\bar{\beta} = \sum_{j=1}^{n} \tau_j \beta_j$

4 $s_{\beta j}$ is the *j*th largest value of the $s_{\alpha i}$.;

5 **Step 2:**Collect all additive linguistic preference relations $R^{(m)}$*(m=1,2,...,l)* into an aggregated linguistic preference relation $\hat{R}$=$(\hat{r}_{ij})_{nxn}$;

6 **Step 3:**In order to aggregate the preference information $(\hat{r}_{ij})$ in the *ith* alternative over all the other alternatives utilise the following operator;

7 z_i=$(\hat{r}_{ij})$=$\frac{1}{m}$ $(\hat{r}_i^{(1)}_j \oplus \hat{r}_i^{(2)}_j \oplus \ldots \oplus \hat{r}_i^{(n)}_j)$;

8 **Step 4:** Rank all the alternative and select the highest valued option from the value of z_i*(i=1,2,...,n)*;

9 **end**

Algorithm 2: Usage of the EIOWA Operator with Trust Values

input : *x_i: set of alternatives (i=1,2,...,n)*
decision makers, $DM_l, l \geq 1$
output: Aggregated Matrix

Preference Process;
for $k \leftarrow 1$ **to** l **do**
  the round for decision makers;
  for $i \leftarrow 1$ **to** n **do**
    the value of the alternative x_i ;
    for $j \leftarrow 1$ **to** n **do**
      s_a *($-q \leq a \leq q$): x_j th x_i value*;
    end
  end
end
Aggregation Process;
τ_{o-dl}: $\tau_1, \tau_2, ..., \tau_l$;
for $k \leftarrow 1$ **to** l **do**
  the round for decision makers;
  for $i \leftarrow 1$ **to** n **do**
    $s_{a/-a}$: *the value of the alternative x_i*;
    for $j \leftarrow 1$ **to** n **do**
      $EIOWA\tau(s_{\alpha 1}, s_{\alpha 2}, ..., s_{\alpha n}) = \tau_1 s_{\beta 1} \otimes \tau_2 s_{\beta 2} \otimes ... \otimes \tau_n s_{\beta n} = s_{\bar{\beta}}$
    end
  end
end

Algorithm 3: Algorithm: Aggregation on x_i

In Algorithm 3, we have given the steps of the EIOWA techniques with the usage of users' trust values. It takes the alternative choices as input values and gives the aggregated matrix as an output. As it is aforementioned, τ is the weighting values for decision makers' opinions in the decision making process. τ is the owner's trust values in each co-owner's where τ ranges in [0,1] (detailed explanation about the trust τ value is given in the next chapter). The most trusted co-owner's opinion has more effect in the co-owned data decision making process, however, it does not mean that others opinions are unimportant. All decision makers opinions are taken into the consideration in the co-owned data sharing process. In the algorithm, taking co-owner's choices is the first step. The second step is weighting decision makers' (*co-owners*) opinions in which trust value τ is used for weighting. The final step is to calculate the aggregated preference relation values.

5.4.2 Best Alternative Selection: DEI-DEO

Decision in-Decision Out (DEI-DEO) is a fusion technique, in which input decisions are fused to obtain either a better or new decision Dasarathy (1997). The DEI-DEO in Figure 5.1 represents the implementation of decision in-decision out technique. The function for the implementation of the technique is given in Equation 5.5, which takes two decisions values from the *Fuzzy Decision System* and the *Fuzzy Alternative System* and provides fused/ best decision D_o. Table 5.1 represents the conditions in order to obtain the fused decision. There are input decision variables D_1, D_2 and there is one decision output D_o variables. D_1 can have only three different values, it is important to highlight that D_1's outputs are same values with fuzzy logic-based decision system's output in Chapter 4.

Table 5.2 shows the values of the output decision expressions (D_o). In order to take the best decision for protecting the data security, the decision taken from both systems

Table 5.1: Decision In-Decision Out Conditional Rules

Condition	**Decision In 1** D_1	**Operator**	**Decision In 2** D_2	**Decision Out** D_o
IF	YES	&	x_1	o_1
IF	YES	&	x_2	o_2
IF	YES	&	x_3	o_3
IF	YES	&	x_4	o_5
IF	MAYBE	&	x_1	o_5
IF	MAYBE	&	x_2	o_2
IF	MAYBE	&	x_3	o_3
IF	MAYBE	&	x_4	o_5
IF	NO	&	x_1	o_5
IF	NO	&	x_2	o_5
IF	NO	&	x_3	o_5
IF	NO	&	x_4	o_4

needs to be consistent, therefore, we have generated the rules which can ensure that the decisions are consistent. o_1, o_2, o_3, and o_4 are the sufficient outputs and show that the consensus is reached by co-owners in the decision making process. However, o_5 has the case which shows the consensus is not reached in the first round, therefore, the second round is required for a group decision. The second round is started by giving a notification to co-owners (see notification box in Figure 5.2).

Table 5.2: The values of Decision Output

D_o	Value	Definition
o_1	x_1	Share with full permissions
o_2	x_2	Share with restrictions
o_3	x_3	Share with no permissions
o_4	x_4	Do not share
o_5	R_c	Reconsider on Choices

- **Case Conflict:** This case happens when the Fuzzy System's Decision (D_1) is in conflict with the Fuzzy Alternative System (D_2). In such cases, DEI-DEO control point's output is o_5, which shows the conflict and gives a recommendation to the

decision makers in order to resolve inconsistency.

For instance, if the D_1 is *NO*, which simply shows the decision makers are worried about their data security features (*CIAPP*), and the D_2 is x_1, then the conflict happens.

In order to resolve the conflicts, we define the model that is given in Equation 5.5. The model is a representation of decision fusion technique. Equation 5.5 is a function that has two input variables, which are D_1 and D_2, and one output variable D_o.

- **Case Convenient:** This case happens when the Fuzzy System's Decision (D_1) and the Fuzzy Alternative System (D_2) are consistent. In such cases, DEI-DEO control point's output is either o_1, o_2, o_3, or o_4.

$$f_t(D_1, D_2) = D_{oi} \qquad \textit{where, } 1 \leq i \leq 5 \tag{5.5}$$

The proposed framework has time restriction, decision makers are supposed to make a consensus-reached decision in time t. If the time is over and the group members have not reached an appropriate decision, then the framework notifies the owner with the last decision that is made in time t. If the last output value of DEI-DEO is o_5 in time t, then it is a special case. If the owner is notified with the o_5 then they can make the decision because of unattainable consensus decision in the group.

Algorithm 4 shows the steps of selection process for the most appropriate decision. When the aggregated preference relation value is taken in Algorithm 3, the decision consistency on outcome of both the fuzzy decision system and the fuzzy alternative system is controlled. In Algorithm 4, D_1 is the output of fuzzy logic-based decision system and D_2 is

the output from the fuzzy alternative system. D_1 and D_2 are taken as input variables and D_o is the output value. The D_o could have five different outputs which is either a consistent output values with x_1, x_2, x_3, x_4 or an inconsistent output value R_c in a specific time t. In OSNs, it is hard to define t due to the social networks' aspects. Time t is negotiation, therefore, we assume that t somehow is defined.

```
1  Selection Process;
   input  : D1, D2
   output: Do, o ∈ {1,2,3,4,5}
2  Time t:
3  for i = 1 to t do
4      Do ← fT1(D1, D2) if o1 then
5          x1 :best alternative;
6      else if o2 then
7          x2 :best alternative ;
8      else if o3 then
9          x3 :best alternative ;
10     else if o4 then
11         x4 :best alternative ;
12     else
13         Recommend: Do5
14         Reconsideration on choices "This data sharing might cause privacy leakage
             for someone";
15     end
16     return: Doi alternative
17 end
18 return: Consensus Not reached
```

Algorithm 4: Algorithm 3: DEI-DEO Functions

5.5 Illustrative Experimental Study

The set of choices X is as follows;

X=

$$\left\{\begin{array}{c} x_1 = \textit{Share with full permission} \\ x_2 = \textit{Share with restrictions} \\ x_3 = \textit{Share with no permission} \\ x_4 = \textit{Do not share} \end{array}\right\}$$

and the linguistic labels are given as follows: S=

$$\left\{\begin{array}{ll} s_{-4} & \text{extremely worried} \Longrightarrow \text{EW} \\ s_{-3}: & \text{very worried} \Longrightarrow \text{VW} \\ s_{-2} & \text{worried} \Longrightarrow \text{W} \\ s_{-1} & \text{slightly worried} \Longrightarrow \text{SW} \\ s_0 & \text{do not mind} \Longrightarrow \text{DNM} \\ s_1 & \text{slightly agree} \Longrightarrow \text{SA} \\ s_2 & \text{agree} \Longrightarrow \text{A} \\ s_3 & \text{fully agree} \Longrightarrow \text{FA} \\ s_4 & \text{extremely agree} \Longrightarrow \text{EA} \end{array}\right\}$$

In order to characterise the fuzzy linguistic terms, given on the above set S, trapezoidal membership functions. Figure 5.3 represents the membership functions ranges with their linguistic values. Each co-owner's choices on the alternative set members, with the given linguistic variables are used to calculate the group decision value if the group members can reach a decision.

Table 5.3, Table 5.4, Table 5.5, Table 5.6, and Table 5.7 present the preference linguistic

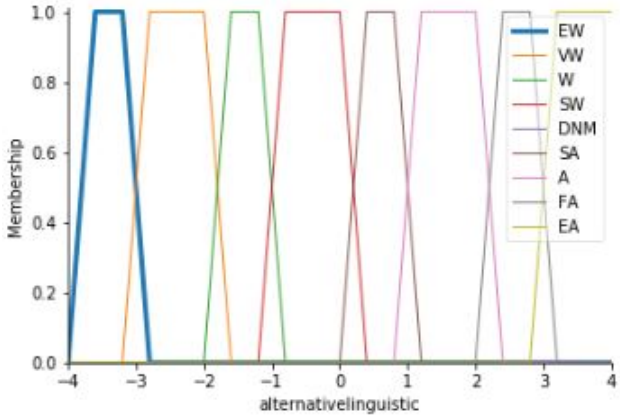

Figure 5.3: Linguistic term set membership functions

variables for each decision maker. On the tables, $s_0, s_1, ..., s_4$ are the numerical values of the preference values. All numerical values are also correlated with their linguistic values from Table 5.5.

Table 5.3: Linguistic Preference Relation R^1

	x_1 Share with full permission	x_2 share with restrictions	x_3 share with no permission	x_4 do not share
x_1	$s_0 \Longrightarrow$ DNM	$s_{-3} \Longrightarrow$ VW	$s_{-4} \Longrightarrow$ EW	$s_{-4} \Longrightarrow$ EW
x_2	$s_3 \Longrightarrow$ A	$s_0 \Longrightarrow$ DNM	$s_2 \Longrightarrow$ A	$s_{-2} \Longrightarrow$ W
x_3	$s_4 \Longrightarrow$ EA	$s_{-2} \Longrightarrow$ W	$s_0 \Longrightarrow$ DNM	$s_3 \Longrightarrow$ FA
x_4	$s_4 \Longrightarrow$ EA	$s_2 \Longrightarrow$ A	$s_{-3} \Longrightarrow$ VW	$s_0 \Longrightarrow$ DNM

Table 5.4: Linguistic Preference Relation R^2

	x_1 Share with full permission	x_2 share with restrictions	x_3 share with no permission	x_4 do not share
x_1	$s_0 \Longrightarrow$ DNM	$s_1 \Longrightarrow$ SA	$s_{-2} \Longrightarrow$ W	$s_{-4} \Longrightarrow$ EW
x_2	$s_{-1} \Longrightarrow$ SW	$s_0 \Longrightarrow$ DNM	$s_1 \Longrightarrow$ SA	$s_{-2} \Longrightarrow$ W
x_3	$s_2 \Longrightarrow$ A	$s_{-1} \Longrightarrow$ SW	$s_0 \Longrightarrow$ DNM	$s_4 \Longrightarrow$ EA
x_4	$s_4 \Longrightarrow$ EA	$s_2 \Longrightarrow$ A	$s_{-4} \Longrightarrow$ EW	$s_0 \Longrightarrow$ DNM

The trust values between the data owner and decision makers are used to weight the decision makers opinions, see Table 5.8. Given trust values are owner's trust in each

Table 5.5: Linguistic Preference Relation R^3

	x_1 Share with full permission	x_2 share with restrictions	x_3 share with no permission	x_4 do not share
x_1	$s_0 \Longrightarrow$ DNM	$s_3 \Longrightarrow$ FA	$s_3 \Longrightarrow$ FA	$s_4 \Longrightarrow$ EA
x_2	$s_{-3} \Longrightarrow$ VW	$s_0 \Longrightarrow$ DNM	$s_{-3} \Longrightarrow$ VW	$s_{-1} \Longrightarrow$ SW
x_3	$s_{-3} \Longrightarrow$ W	$s_3 \Longrightarrow$ FA	$s_0 \Longrightarrow$ DNM	$s_2 \Longrightarrow$ A
x_4	$s_{-4} \Longrightarrow$ EW	$s_1 \Longrightarrow$ SA	$s_{-2} \Longrightarrow$ W	$s_0 \Longrightarrow$ DNM

Table 5.6: Linguistic Preference Relation R^4

	x_1 Share with full permission	x_2 share with restrictions	x_3 share with no permission	x_4 do not share
x_1	$s_0 \Longrightarrow$ DNM	$s_2 \Longrightarrow$ A	$s_{-3} \Longrightarrow$ VW	$s_4 \Longrightarrow$ EA
x_2	$s_{-2} \Longrightarrow$ W	$s_0 \Longrightarrow$ DNM	$s_2 \Longrightarrow$ A	$s_{-2} \Longrightarrow$ W
x_3	$s_3 \Longrightarrow$ FA	$s_{-2} \Longrightarrow$ W	$s_0 \Longrightarrow$ DNM	$s_3 \Longrightarrow$ FA
x_4	$s_{-4} \Longrightarrow$ EW	$s_2 \Longrightarrow$ A	$s_{-3} \Longrightarrow$ VW	$s_0 \Longrightarrow$ DNM

Table 5.7: Linguistic Preference Relation R^5

	x_1 Share with full permission	x_2 share with restrictions	x_3 share with no permission	x_4 do not share
x_1	$s_0 \Longrightarrow$ DNM	$s_1 \Longrightarrow$ SA	$s_{-2} \Longrightarrow$ W	$s_{-4} \Longrightarrow$ EW
x_2	$s_{-2} \Longrightarrow$ W	$s_0 \Longrightarrow$ DNM	$s_1 \Longrightarrow$ SA	$s_{-2} \Longrightarrow$ W
x_3	$s_2 \Longrightarrow$ A	$s_{-1} \Longrightarrow$ SW	$s_0 \Longrightarrow$ DNM	$s_{-4} \Longrightarrow$ EW
x_4	$s_4 \Longrightarrow$ EA	$s_2 \Longrightarrow$ A	$s_4 \Longrightarrow$ EA	$s_0 \Longrightarrow$ DNM

co-owner.

Table 5.8: Owner's trust in decision makers (τ_{o-dl})

DM_l	The trust value τ_{o-d_l}
DM_1	0.01
DM_2	0.01
DM_3	0.03
DM_4	0.03
DM_5	0.02

Utilising the *EIOWA* operator is done by taking the following step;

$\hat{r}_{ij}$=*EIOWAw* ($r_{ij}{}^{(1)}$,$r_{ij}{}^{(2)}$,...,$r_{ij}{}^{(m)}$)

τ represents the trust values that exist between decision makers in data owner, $\tau = T_o - {}_{co}$. We take the parameter values a=0.5, b=0.5 and the values of the weights become w=*0.5,0.5*.

τ_1=0.01 and τ_2=0.01, τ_3=0.03,τ_4=0.03,τ_5=0.02 .

Table 5.9 and Table 5.10 include detailed explanation of the EIOWA technique calculation. Each value on the linguistic tables are used to create the aggregation matrix in Table 5.9. Result values on Table 5.10 are then used to create aggregated preference relation.

Table 5.11 is the aggregation preference relation which is created with the result of Table 5.10. As it is seen there are four alternatives in the table and it is still a matrix. However, the values i each cells are not the same values that are given in the linguistic values. This is because these values are aggregated values from each preferences taken from each co-owner. After aggregating the preference relation, it is needed to compute the degree of the global preference. Therefore, the next step is to make the averaged preference degree, see Table 5.12.

Once the preference degrees are averaged, all the alternatives are ranked in accordance

Table 5.9: Calculation for the aggregation matrix

Details of Calculation for Each Value on The Aggregation Matrix
$\hat{r}_{11}=\tau_1 x {R^1}_{11} \otimes \tau_2 x {R^2}_{11} \otimes \tau_3 x {R^3}_{11} \otimes \tau_4 x {R^4}_{11} \otimes \tau_5 x {R^5}_{11}$
$\hat{r}_{12}=\tau_1\ {R^1}_{12} \otimes \tau_2\ x {R^2}_{12} \otimes \tau_3 x {R^3}_{12} \otimes \tau_4 x {R^4}_{12} \otimes \tau_5 x {R^5}_{12}$
$\hat{r}_{13}=\tau_1 x {R^1}_{13} \otimes \tau_2 x {R^2}_{13} \otimes \tau_3 x {R^3}_{13} \otimes \tau_4 x {R^4}_{13} \otimes \tau_5 x {R^5}_{13}$
$\hat{r}_{14}=\tau_1 x {R^1}_{14} \otimes \tau_2 x {R^2}_{14} \otimes \tau_3 x {R^3}_{14} \otimes \tau_4 x {R^4}_{14} \otimes \tau_5 x {R^5}_{13}$
$\hat{r}_{21}=\tau_1 x {R^1}_{21} \otimes \tau_2 x {R^2}_{21} \otimes \tau_3 x {R^3}_{21} \otimes \tau_4 x {R^4}_{21} \otimes \tau_5 x {R^5}_{21}$
$\hat{r}_{22}=\tau_1 x {R^1}_{22} \otimes \tau_2 x {R^2}_{22} \otimes \tau_3 x {R^3}_{22} \otimes \tau_4 x {R^4}_{22} \otimes \tau_5 x {R^5}_{22}$
$\hat{r}_{23}=\tau_1 x {R^1}_{23} \otimes \tau_2 x {R^2}_{23} \otimes \tau_3 x {R^3}_{23} \otimes \tau_4 x {R^4}_{23} \otimes \tau_5 x {R^5}_{23}$
$\hat{r}_{24}=\tau_1 x {R^1}_{24} \otimes \tau_2 x {R^2}_{24} \otimes \tau_3 x {R^3}_{24} \otimes \tau_4 x {R^4}_{24} \otimes \tau_5 x {R^5}_{24}$
$\hat{r}_{31}=\tau_1 x {R^1}_{31} \otimes \tau_2 x {R^2}_{31} \otimes \tau_3 x {R^3}_{31} \otimes \tau_4 x {R^4}_{31} \otimes \tau_5 x {R^5}_{31}$
$\hat{r}_{32}=\tau_1 x {R^1}_{32} \otimes \tau_2 x {R^2}_{32} \otimes \tau_3 x {R^3}_{32} \otimes \tau_4 x {R^4}_{32} \otimes \tau_5 x {R^5}_{32}$
$\hat{r}_{33}=\tau_1 x {R^1}_{33} \otimes \tau_2 x {R^2}_{33} \otimes \tau_3 x {R^3}_{33} \otimes \tau_4 x {R^4}_{33} \otimes \tau_5 x {R^5}_{33}$
$\hat{r}_{34}=\tau_1 x {R^1}_{34} \otimes \tau_2 x {R^2}_{34} \otimes \tau_3 x {R^3}_{34} \otimes \tau_4 x {R^4}_{34} \otimes \tau_5 x {R^5}_{34}$
$\hat{r}_{41}=\tau_1 x {R^1}_{41} \otimes \tau_2 x {R^2}_{41} \otimes \tau_3 x {R^4}_{41} \otimes \tau_4 x {R^4}_{41} \otimes \tau_5 x {R^5}_{41}$
$\hat{r}_{42}=\tau_1 x {R^1}_{42} \otimes \tau_2 x {R^2}_{42} \otimes \tau_3 x {R^4}_{42} \otimes \tau_4 x {R^4}_{42} \otimes \tau_5 x {R^5}_{42}$
$\hat{r}_{43}=\tau_1 x {R^1}_{43} \otimes \tau_2 x {R^2}_{43} \otimes \tau_3 x {R^4}_{43} \otimes \tau_4 x {R^4}_{43} \otimes \tau_5 x {R^5}_{43}$
$\hat{r}_{44}=\tau_1 x {R^1}_{44} \otimes \tau_2 x {R^2}_{44} \otimes \tau_3 x {R^4}_{44} \otimes \tau_4 x {R^4}_{44} \otimes \tau_5 x {R^5}_{44}$

Table 5.10: Each value of calculation for the aggregation matrix

Details of the Calculation	Result Value
$\hat{r}_{11}=0.01 x s_0 \otimes 0.01 x s_0 \otimes 0.03 x s_0 \otimes 0.03 x s_0 \otimes 0.02 x s_0$	$\hat{r}_{11}$ =0
$\hat{r}_{12}=0.01 x s_{-3} \otimes 0.01 x s_1 \otimes 0.03 x s_3 \otimes 0.03 x s_2 \otimes 0.02 x s_1$	$\hat{r}_{12}$ =0.15
$\hat{r}_{13}=0.01 x s_{-4} \otimes 0.01 x s_{-2} \otimes 0.03 x s_3 \otimes 0.03 x s_{-3} \otimes 0.02 x s_{-2}$	$\hat{r}_{13}$ =-0.1
$\hat{r}_{14}=0.01 x s_{-4} \otimes 0.01 x s_{-4} \otimes 0.03 x s_4 \otimes 0.03 x s_4 \otimes 0.02 x s_{-4}$	$\hat{r}_{14}$ =0.08
$\hat{r}_{21}=0.01 x s_3 \otimes 0.01 x s_{-1} \otimes 0.03 x s_{-3} \otimes 0.03 x s_{-2} \otimes 0.02 x s_{-2}$	$\hat{r}_{21}$ =-0.17
$\hat{r}_{22}=0.01 x s_0 \otimes 0.01 x s_0 \otimes 0.03 x s_0 \otimes 0.03 x s_0 \otimes 0.02 x s_0$	$\hat{r}_{22}$ =0
$\hat{r}_{23}=0.01 x s_2 \otimes 0.01 x s_1 \otimes 0.03 x s_{-3} \otimes 0.03 x s_2 \otimes 0.02 x s_2$	$\hat{r}_{23}$ =0.04
$\hat{r}_{24}=0.01 x s_{-2} \otimes 0.01 x s_{-2} \otimes 0.03 x s_{-1} \otimes 0.03 x s_{-2} \otimes 0.02 x s_{-2}$	$\hat{r}_{24}$ =-0.17
$\hat{r}_{31}=0.01 x s_4 \otimes 0.01 x s_2 \otimes 0.03 x s_{-3} \otimes 0.03 x s_3 \otimes 0.02 x s_2$	$\hat{r}_{31}$ =0.1
$\hat{r}_{32}=0.01 x s_{-2} \otimes 0.01 x s_{-1} \otimes 0.03 x s_3 \otimes 0.03 x s_{-2} \otimes 0.02 x s_{-1}$	$\hat{r}_{32}$ =-0.02
$\hat{r}_{33}=0.01 x s_0 \otimes 0.01 x s_0 \otimes 0.03 x s_0 \otimes 0.03 x s_0 \otimes 0.02 x s_0$	$\hat{r}_{33}$ =0
$\hat{r}_{34}=0.01 x s_3 \otimes 0.01 x s_4 \otimes 0.03 x s_2 \otimes 0.03 x s_3 \otimes 0.02 x s_{-4}$	$\hat{r}_{34}$ =0.14
$\hat{r}_{41}=0.01 x s_4 \otimes 0.01 x s_4 \otimes 0.03 x s_{-4} \otimes 0.03 x s_{-4} \otimes 0.02 x s_4$	$\hat{r}_{41}$ =-0.08
$\hat{r}_{42}=0.01 x s_2 \otimes 0.01 x s_2 \otimes 0.03 x s_1 \otimes 0.03 x s_2 \otimes 0.02 x s_2$	$\hat{r}_{42}$ =0.17
$\hat{r}_{43}=0.01 x s_{-3} \otimes 0.01 x s_{-4} \otimes 0.03 x s\_2 \otimes 0.03 x s_{-3} \otimes 0.02 x s_4$	$\hat{r}_{43}$ =-0.14
$\hat{r}_{44}=0.01 x s_0 \otimes 0.01 x s_0 \otimes 0.03 x s_0 \otimes 0.03 x s_0 \otimes 0.02 x s_0$	$\hat{r}_{44}$ =0

Table 5.11: Aggregated preference relation R

	x_1	x_2	x_3	x_4
x_1	0	-0.14	-0.11	-0.08
x_2	0.14	0	0.08	-0.05
x_3	0.11	-0.08	0	0.01
x_4	0.08	0.05	-0.1	0

Table 5.12: The averaged preference degree

$\frac{\sum_{n=1}^{4} x_{1n}}{4}$	-0.082
$\frac{\sum_{n=1}^{4} x_{2n}}{4}$	0.042
$\frac{\sum_{n=1}^{4} x_{3n}}{4}$	0.01
$\frac{\sum_{n=1}^{4} x_{4n}}{4}$	0.007

with the values of r_i *(i=1,2,3,4)*.

Table 5.13: Ranked alternatives

$z_2 > z_3 > z_4 > z_1$
$x_2 > x_3 > x_4 > x_1$

When the ranking process is finished, the Fuzzy Alternative System's decision is transferred to the DEI-DEO functions to check whether Fuzzy System's and Fuzzy Alternative System's decisions' are convenient.

DEI-DEO Result

The results of Fuzzy Decision System and Fuzzy Alternative System are checked based upon the conditions that are given in Table 5.2 and Table 5.1. If an appropriate decision is made at time t, then the owner is notified with the D_{oi} and share the data with permission

X_i. After the data sharing process is completed, the trust values of decision makers' on owner are updated. If the decision X_i is equal to the R_c, after the time t, then the owner decides to share the data with his permission. If the group could not reach a consensus decision, then the trust values of co-owners' is not updated.

Table 5.14: Consensus Decision during time t

FDS's out	FAS's out	Degree	CRP_{dec}
maybe	x_4	0.35	$x_4 > x_2 > x_1 > x_3$

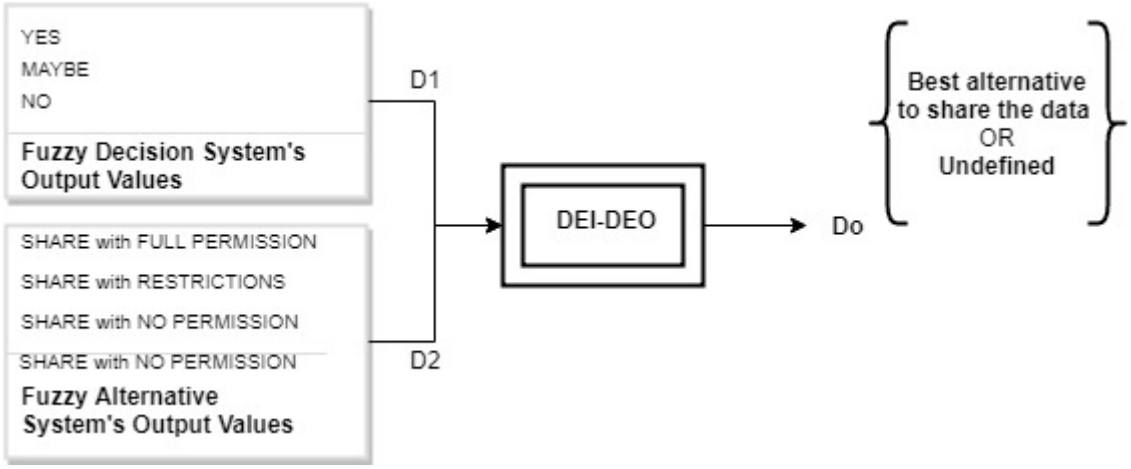

Figure 5.4: Selection of the best alternative

5.6 Conclusion

The applicability and the usability of group decision making in OSNs has been an issue in the literature as it is mentioned in Chapter 2. The proposed consensus-reached group decision making system in this chapter not only filled that gap in the literature but also introduces the usability of users' trust values to weights users opinions in a co-owned data sharing process. A group decision making or more specifically a consensus-reached group decision making was an issue in OSNs because of the way for weighting decision

makers' opinion in a decision making process. This thesis solved this problem with the usage of trust values. Used trust values are calculated with novel and robust equations. None of the previous works in the area of group decision making used trust values because there was not such trust models which can be used to calculate users' trust values.

The consensus-reached decision is a need in OSNs' platforms especially in co-owned data sharing processes. Because co-owned data belongs to more than one user, who are involved in the content of data, have a right to express their opinions in co-owned data sharing processes. It is also necessary to have more secure co-owned data sharing processes in OSNs. With the proposed consensus-reached group decision making process, co-owners are given a chance to express their opinions in the sharing process in which any privacy concerns can be expressed.

In this chapter, a consensus-based group decision model has been presented for co-owned data sharing in OSNs. In the proposed CRP co-owned data sharing process, group members (DMs) are expected to reach a consensus-reached decision in a certain time. If the group members can not reach a consensus decision within the given time, then the data owner is notified with *Undefined* case. In such a case, the data owner makes the decision for sharing the data.

The consensus has been reached based on the decision fused technique's output. If the group members decisions taken from *Fuzzy Decision System* and *Fuzzy Alternative System* are convenient decisions, then the output of the DEI-DEO is given to the data owner. Otherwise, group members are asked to reconsider their choices to reach an appropriate decision in a certain time, which does not cause conflict between *Fuzzy Decision System* output and *Fuzzy Alternative System* output.

We have used the trust values to weight each decision makers' opinions in the given

model. The trust values are updated based on the owner's action on co-owned data sharing process if the decision makers can give an appropriate decision within the prescribed time. Otherwise, the trust values are not changed because of the conflicts among decision makers' opinions.

In the model, the data owner is the moderator who makes the final decision in the sharing processes. There are two options for the moderator; he can either respects co-owners' group decision and share the content with the group's decision or make his/her own decision with disrespect to the group's members' decision. In both cases, there should be a discipline in OSNs which should be able to show the appreciation and reprimand. In the next chapter, we will explain how award and punishment can be applied in co-owned data sharing processes in OSNs.

Chapter 6

Using Users' Trust and Reputation Values in Co-owned Data Sharing Processes

This chapter introduces trust models and reputation models which are used in co-owned data sharing processes in OSNs. In Chapter 5, we addressed the need for trust values and the reputation values in OSNs. This part of the thesis answers several research questions discussed previously and also formally introduces the trust model and the reputation model for OSNs.

Analysing and understanding of the importance of trust values in OSNs and analysing the effective features on the trust and reputation models are important in developing the trust model and the reputation models which are used in co-owned data sharing processes in OSNs in this thesis. Sharing information is an important part of life but the difficult part of the sharing process is to decide that with whom data should be shared Talja and Hansen

(2006). Because, sometimes shared information could cause profound impacts on other people' lives. In such a case, people lose trust in other person who affects their lives in a bad way. With this respect, we develop trust models among OSNs' users.

6.1 Understanding Trust Modelling in OSNs

In OSNs, trust is defined as a direct connection from one user to another user Jiang et al. (2016). It is usually considered that if there is an edge (*i.e. relationship*) between two nodes (*i.e. users*), then the trust values is equal to 1, otherwise 0. Wang and Wu (2011). With this respect, it is clear that the relationship or direct connection is one of the effective factors in trust understanding in OSNs. Rathore and Tripathy (2017) have evaluated the trust values in OSNs and they have shown that the privacy loss affects trust values in OSNs. The privacy loss has been related to the data sensitivity in Aghasian et al. (2017), however, they have scored the sensitivity value with a general attribute table. OSNs' trust have been connected to the users' relationships and the privacy loss in Xu et al. (2018) and they also have shown that the data sensitivity has an effect in the privacy loss. However, they have claimed that the data sensitivity is a single-handed value which means that the user who uploads the content of data to OSNs is the only person to decide the sensitivity. As it has been addressed in Chapter 4, each person who is involved in the data sharing process could have different concerns on the data. Thus, the data sensitivity needs be decided by the users who have the right on data (see Equation 4.1 in Chapter 4). By considering those requirements, we have developed a trust model with the dependent models which are data sensitivity, privacy loss, and relationship.

Figure 6.1 represents the dependent models to develop the trust and reputation models for this thesis. The starting point is the calculation of the *relation values* and *data sensitiv-*

ity value, which are explained in Chapter 4. With the dependency of these models, the privacy loss value is calculated. Privacy loss is very important value in co-owned data sharing process because the backbone of the privacy issues in OSNs is leakage of privacy. We then develop trust models by relating the privacy loss model. If the privacy loss is equal to 0, then the developed framework calculates the trust gain not trust loss value. More explanation of the relation between models and the dependency are explained when development of privacy loss, trust model, and reputation model are explained in this thesis.

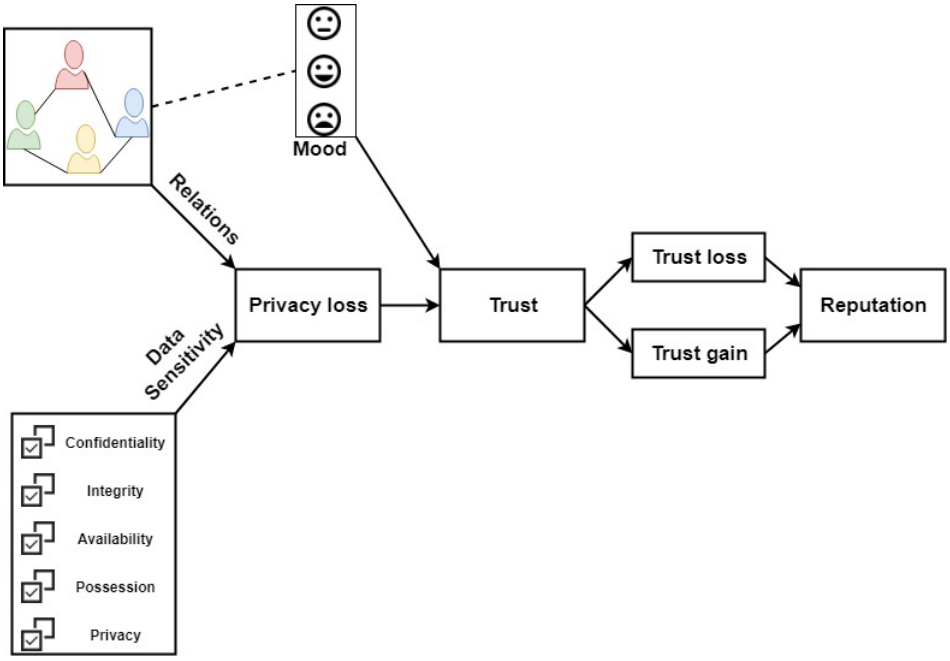

Figure 6.1: Model Developments with Dependency of Models

- **Privacy Loss:** Privacy preserving is protecting the shared data from unauthorised users in OSNs Siddula et al. (2018). The privacy loss can be defined by reversing the privacy protection definition. The privacy loss means that the data is accessed by someone who should not have access to data. Privacy loss is individual/ personal value in OSNs. Each user is given a profile to keep their personal assets.

When a user's personal information is accessed by an unauthorised user, it causes the privacy leakage in OSNs Ali et al. (2018). This is mostly seen in co-owned data sharing in OSNs. By considering these needs, we develop a privacy loss model for co-owned data sharing processes in OSNs. Equation 6.1 presents the privacy loss for each co-owner in a co-owned data sharing process. This equation illustrates that if the owner posts the data without respecting a co-owner's opinion in the co-owned sharing process, especially when a co-owner has concerns on the data security features, then the co-owner will suffer a privacy loss because of the sharing process. In the equation, $R_{(}co_{si)}$ indicates the relation value which exists between each co-owner and targeted group of people. In order to calculate $R_{(}co_{si)}$ value, the existing relationship (*i.e. friendship in OSNs*) is checked. $R_{(}o_{si)}$ shows the relation value between the owner and people in the targeted group.

The model is as follows below;

$$
\begin{aligned}
P_l(c_{owner}) = S_d * |\frac{R_{(}co_{si)}}{R_{(}o_{si)}}| \\
where, \\
|\frac{R_{co_i}{}'}{R_{ci}}| : commonfriends \\
S_d : co-owneddatasensitivity
\end{aligned}
\tag{6.1}
$$

Figure 6.2, 6.3 presents the behaviour of privacy model (Model 6.1) with the changes on the relationship, where the difference between the owner's connections and each co-owner's connections and data sensitivity value (S_d) is calculated. In figures, we hold the line on the relationship value $|\frac{R_{co_i}{}'}{R_{ci}}|$ but vary the sensitivity values. Based on the figures' behaviours, it is important to highlight that when the data sensitivity increases, the privacy loss increases. Given figures are generated with simulated

data. The simulated data reflect the real data; it is checked when the implementation phase of the thesis completed.

- In OSNs, people become unfriend with people who cause privacy leakage on their personal information with sharing data Ahmed et al. (2019), because they do not trust those people for the future interaction. The privacy loss is used to shape the person's trust in another person Richards and Hartzog (2015). This shows us that the privacy loss value has effect on the trust values Akkuzu et al. (2019c).

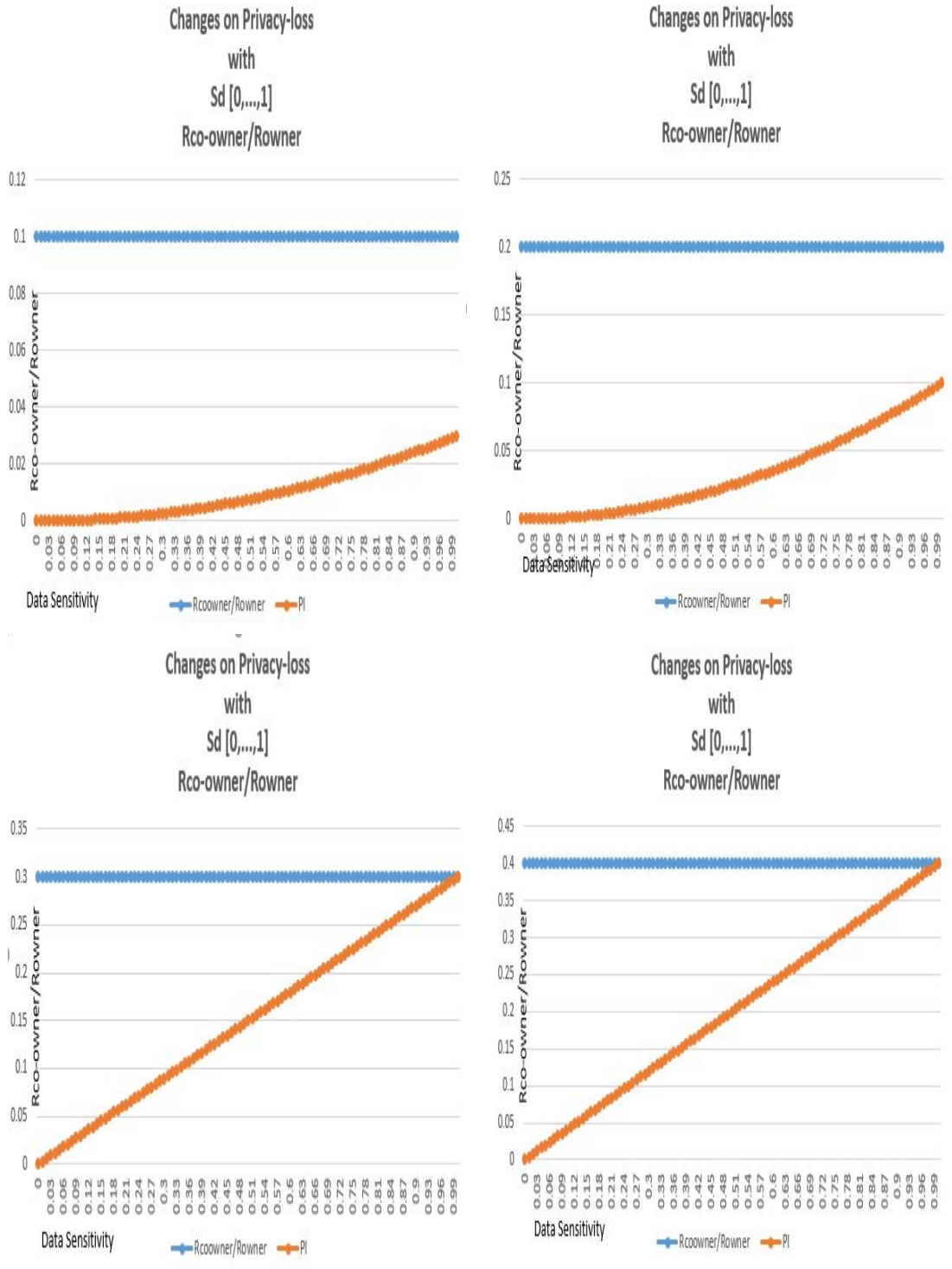

Figure 6.2: Privacy-loss Model Behaviours with Changes on Its Variables

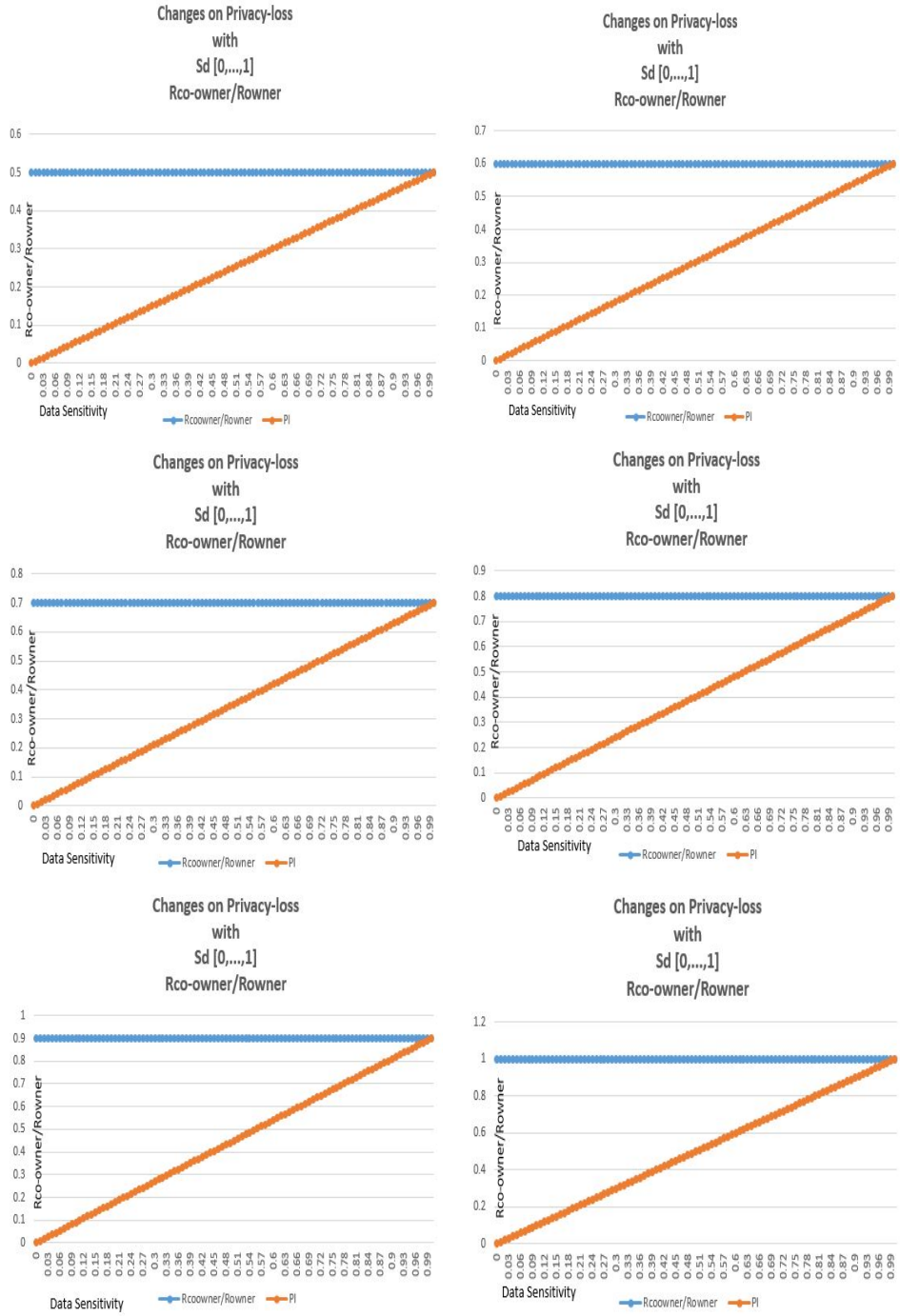

Figure 6.3: Continued:Privacy-loss Model Behaviours with Changes on Its Variables

As it is aforementioned, trust τ plays a key role in co-owned data decision making process. For any users $user_i$ and $user_j$, if they are directly connected (i.e. be friends) where $R_{useri-userj}$=1, we use $\tau_{useri-userj} \in [0,1]$. The more $user_i$ trusts $user_j$, the higher the τ_{useri}-τ_{userj} is. In this work, we have two types of users in a co-owned data sharing process namely the owner and co-owners. Model 6.2 is the representation of trust values between owner and co-owners. These trust values between those pairs are updated, based on the owner's final decision in the sharing process. For example, if the owner respects the decision makers' group decision, then the owner gains trust in co-owners. On the contrary, the owner loses trust in co-owners. In Model 6.2, τ_{ui-uj} indicates $user_i$'s trust in $user_j$ Akkuzu et al. (2019a). Trust has two models trust-loss ($\tau_l(user_i)$) and trust-gain ($\tau_g(user_i)$). The reason for having trust-gain and trust-loss models is to show whether the owner protects or leaks a co-owner's privacy in a co-owned data sharing process. In the trust loss model, we use the exponential function e, which is used to indicate the growth of trust loss with the privacy loss (for more details about the exponential functions Harel and Confrey (1994)). For example, a $user_i$ keeps behaving in a bad way against a $user_j$, the exponential function helps to reduce the $user_j$'s trust decrements in $user_i$. Trust gain model represents the trust values increment between users. Trust gain and trust loss values have been used as feedback values which has been explained in the following section.

$$
\begin{aligned}
\tau_{ui-uj} &\in [0,...,1] \\
(\tau_o) - (\tau_{coi}) &: Owner - trust - in - Co - owner_i \\
(\tau_{coi}) - (\tau_o) &: Co - owner_i - trust - in - Owner \\
\tau_l(user_i) : \tau_l(pl) &= \frac{1 - e^{(pl)}}{1 + e^{(pl)}} \\
\tau_g(user_i) : \tau_{g(\tau ui)} &= (\tau_{ui})^n \qquad (6.2) \\
where, & \\
n_{mood} &= (0 \leq n \leq 1 \\
\tau_l(user_i) &: Trustloss \\
\tau_g(user_i) &: Trustgain
\end{aligned}
$$

Figure 6.4 represents the trust-loss model (see Model 6.2) behaviours depending upon the privacy-loss values. More privacy-loss value causes more loss in trust values. It is apparent that the larger the growth on the privacy loss value, which is the base of the exponential function, the more is the increment on trust loss value. From the data in Figure 6.4, it is apparent that the trust loss values do not go down to -1. This is important because trust-loss and trust gain values are used to calculate a user's reputation value. The higher privacy loss value causes more loss on the trust loss value. Figure 6.5 presents the behaviour of trust gain model in Equation 6.2 with mood value changes and previous trust value. The previous (*i.e. old trust value)* is used to calculate the next trust gain values in order to increase the trust value. From Figure 6.5, it can be seen that trust gain values do not go up to 1.

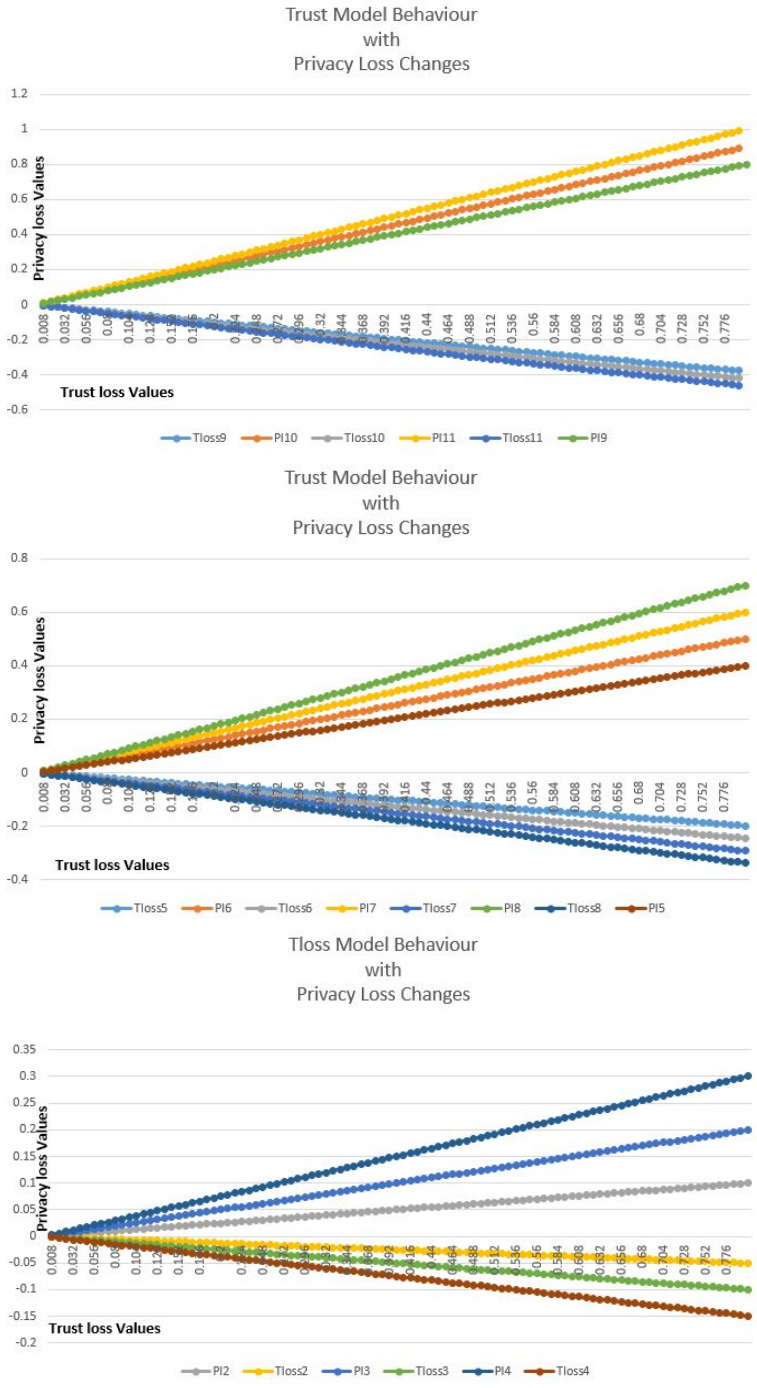

Figure 6.4: Trust-loss Model' Behaviours with Various Privacy-Loss Values

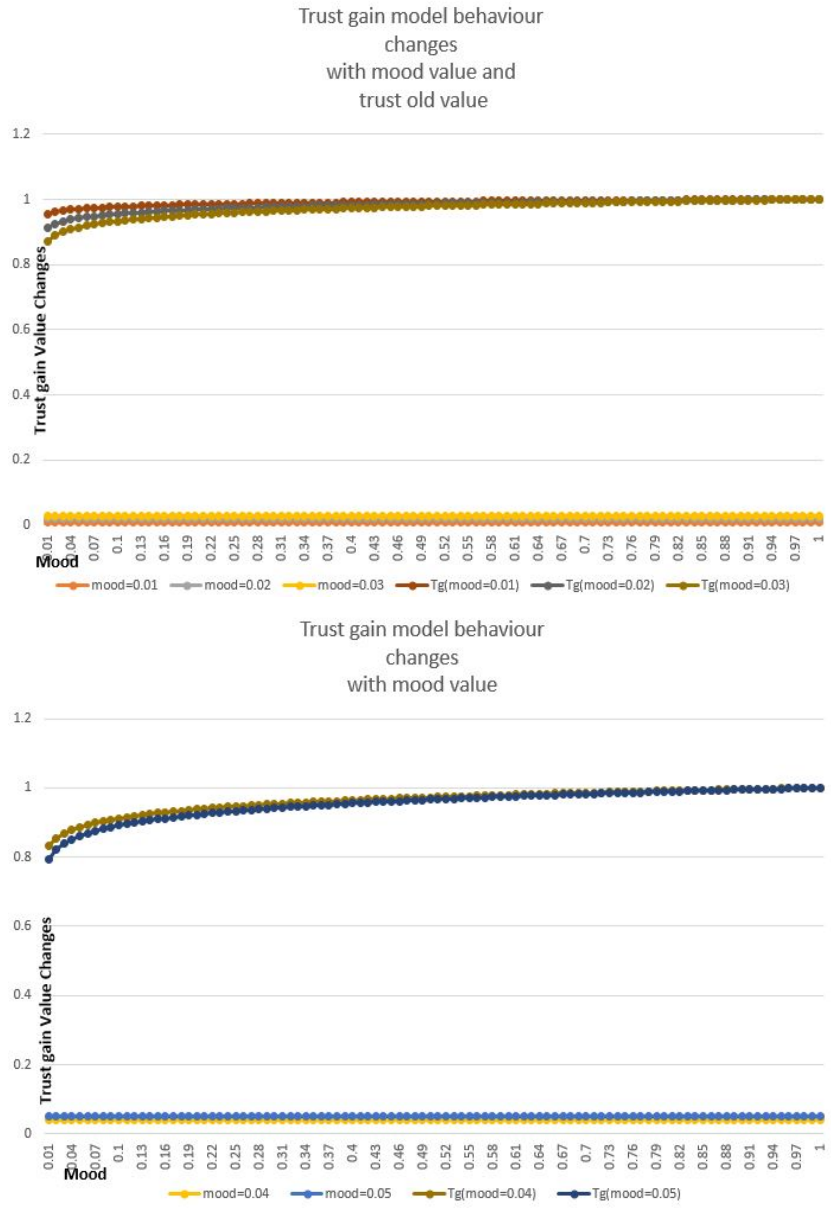

Figure 6.5: Trust-gain Model' Behaviours with Mood and Previous Trust value

6.2 Reputation Modelling with Trust Values for Co-owned Data Sharing Process

In the previous section, we have explained the trust model development steps and the variables which have their contribution in the trust model development. It has also been shown that how the trust model behaves with the changes of variables. In this section, we will show how those trust models can be used in co-owned data sharing processes in OSNs. Trust values increase or decrease based on users' actions in co-owned data sharing processes in OSNs. In other words, after each co-owned data sharing process is completed, each co-owner loses or gains trust in owner. Losing trust in a user points that the owner takes a decision at the end of the sharing process and this sharing causes a privacy loss for a co-owner. However, gaining trust in a user shows the case that the owner's decision was coherent to a co-owners' decision in the data sharing process, which means that sharing co-owned data did not cause any privacy leakage for the co-owner. Therefore, trust values can be considered as feedback values similar to the work in Josang and Ismail (2002). The trust gain value is considered as a satisfaction which illustrates positive feedback while trust lose value is the representation of the dissatisfaction and is seen as a negative feedback. The purpose of having trust values as feedback values is to indicate an owner's punishment or reward in data sharing process, for example, the owner respects co-owners' group decision and it shows that the data sharing process is completed with the satisfaction or vice versa.

Figure 6.6 gives a view to represent trust values among users in OSNs. When a user becomes friend with another user in ONSs, the relationship between these two users appears. In the figure, dashed lines between users represents the relationship. We assume that when users become friends with each other, trust values are automatically assigned

by the system (OSNs). In any OSN platform which uses the developed framework, the trust values are automatically assigned. For instance, τ_{C-A} is the presentation of User C's trust in User A and τ_{A-C} shows User A's trust in User C.

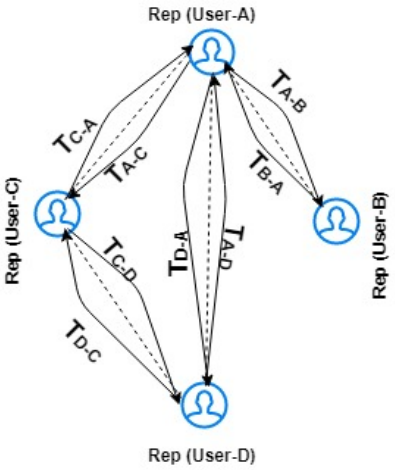

Figure 6.6: An example of representation of trust structure among members

Parameter v is the representation of feedback in Josang and Ismail (2002). In this work, co-owners' trust gain τ_g and trust loss τ_l in owner are used as feedback values. For instance, if co-owners lose trust in the owner, then the value of v trust loss τ_l is (negative), if not then it is trust gain τ_g. The ranges of the variables' values of the model are given in Table 6.1. The table also represents the similarities of the reputation system's variables in Josang and Ismail (2002) and the proposed work's variables for the reputation values. Figure 6.7 depicts the structural representation of the reputation and trust values in OSNs,

Table 6.1: Similarities between the reputation system and OSNs' variables

The reputation system	OSNs' Variables
feedback [-1,1]	Trust values [-1,1]
weights [0,1]	Data sensitivity [0,1]
n $\in \mathbb{N}$	n $\in \mathbb{N}$
is the number of feedback	number of the co-owners

where all users, who are connected to each other, have assigned trust values in each others

and all users in OSNs are assigned a reputation value. It also shows that the changes on the trust values affect the reputation values.

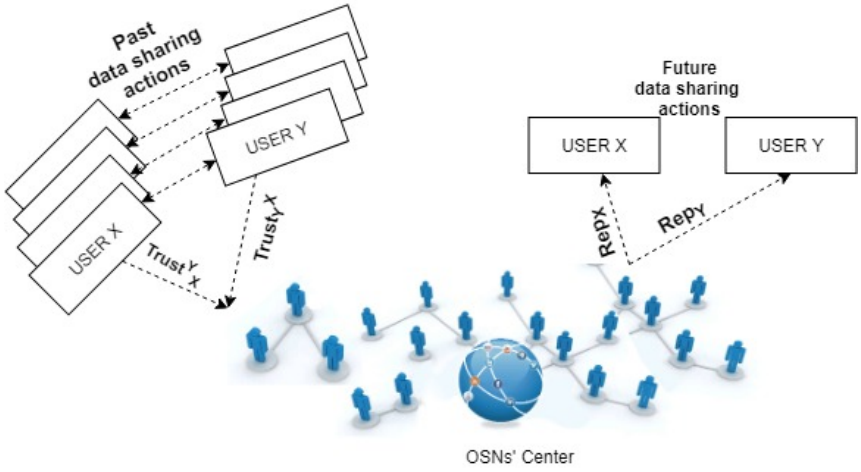

Figure 6.7: Structure of feedback and reputation ratings for OSNs

A general model to calculate the reputation rating of a user in social networks area is defined by Josang Josang and Ismail (2002). The reputation value of a user is calculated by collecting other users' feedback based on his reactions. In the commercial websites, for instance, if a user was satisfied by another user's actions such as buying or selling, then he gives a positive feedback about the user. While users express their unhappiness with negative feedback, which is defined as dissatisfaction variable in Josang and Ismail (2002). Similarly, losing trust and gaining trust in a person could be seen as feedback values in this research. With the trust loss and trust gain values, it is possible to calculate a user's reputation.

We now give our models which are used to calculate reputation value when there is either only trust loss, only trust gain, or trust loss and trust gain. Equation 6.3 is the model that gives the general model for calculating the reputation value with the satisfaction ${c_{co}}^{o}$,

which is trust gain value, and dissatisfaction ${d_{co}}^o$ that is trust loss value.

$$Rep({c_{co}}^o, {d_{co}}^o) = \frac{{c_{co}}^o - {d_{co}}^o}{{c_{co}}^o + {d_{co}}^o + 2} \tag{6.3}$$

Model 6.4 is the representation of of Model 6.3 with only data sensitivity value and the number of co-owners. *Sd* is the data sensitivity value which is used as weight since the data sensitivity value is the expression of co-owners' opinion on the data security features. The data sensitivity value can have the highest value 1 when all of data security features are selected by co-owners as they do get worry on the co-owned data sharing process. In other words, the data sensitivity values gets the highest value when all the data security features are selected by co-owners. All these cases are shown in the following figures.

$$Rep = \frac{n * Sd}{n * Sd + 2} \tag{6.4}$$

The behaviour of Model 6.4 should be presented with varying the data sensitivity value S_d. Let the owner loses trust in co-owners which implies data sensitivity value. The reputation model is a function of the number of co-owners n and data sensitivity in a co-owned data sharing process. The expectation is that when the data sensitivity has the highest value, the changes on the reputation value should get the highest changes. Also the model should be able to calculate the reputation value when there is no trust loss value but trust gain value is exist. This is the simplest model of the reputation, however, it needs more variable for calculating changes on a user's reputation value. Because, in a co-owned data sharing trust loss and trust gain values are important variables. Therefore, trust loss and trust gain values need to be used in the reputation model calculation. In order to do so, we developed the next reputation model in which trust loss and trust gain values are used in the reputation calculation.

Model 6.5 is the representation of a normalised form of Model 6.3 with satisfaction c and dissatisfaction d, respectively. Sd is the data sensitivity value which is used as weight since the data sensitivity value is the expression of co-owners' opinion on the data security features. $c \in [0,1]$ and $d \in [-1,0]$. The trust value can have the highest value $\tau_g = 1$ when none of data security features are selected by co-owners as they do not worry on the sharing process, while it carries the minimum value $\tau_l = -1$, when all the data security features are selected by co-owners. It is important to note that from this point, all the equations are developed on top of this model.

$$\begin{aligned} c &= \frac{Sd * (1+\tau_g)}{2} \\ d &= \frac{Sd * (1-\tau_l)}{2} \end{aligned} \tag{6.5}$$

Model 6.6 indicates the calculation of the reputation value when there is no trust loss τ_l value and no data sensitivity S_d value. In the model, c is the representation of trust gain τ_g and d is the representation of trust loss τ_l value. When there is no trust loss value and $\tau_l = 0$, the reputation value is calculated with only trust gain τ_g and the number of co-owners n, who do not have any concerns on data security features and are happy to share intended data with targeted group.

$$\begin{aligned} c : \mathbb{R}, d : \mathbb{R} \\ Rep : cXd; \\ Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \\ c = \frac{(1+\tau_g)}{2}, \\ d = 0, \\ Rep(c_i, 0) = n * \frac{c}{c+2} \\ Rep(c, 0) = \frac{\sum_{i=1}^{n} Rep(c_i, 0)}{n} \end{aligned} \tag{6.6}$$

Figure 6.8 indicates the changes on the reputation model with Equation 6.6. The model has two input inconstant variables τ_g *and* n, and constant variables come from Model 6.4. In the figure, we have shown the behaviours of Model 6.6 by changing the number of co-owners and trust gain τ_g variable's values. In the figure, we have pointed some random reputation values Rep_{ci} with trust gain τ_g points and the number of people n, the last reputation value Rep with summation of Rep_i values and dividing it with total number of co-owners n. The expectation from the model is that the model needs to increase a user's reputation value. When Figure 6.8 is checked closely; it can be clearly seen that the reputation value consistently increases by the increment of trust gain values. The increment on the reputation value demonstrates the model (Equation 6.6) meets expected behaviour.

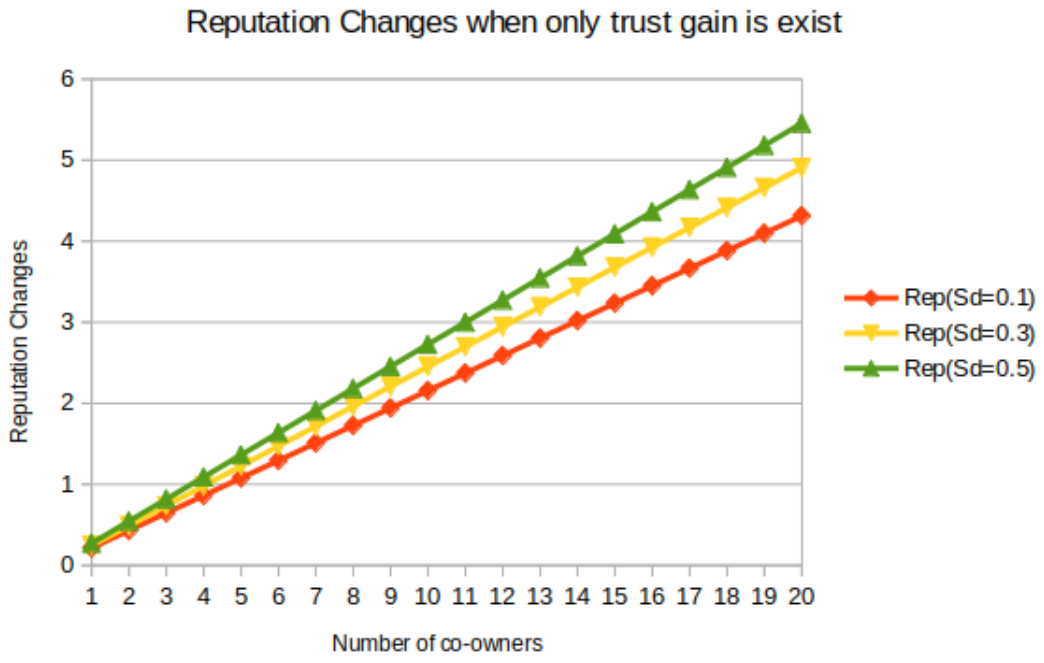

Figure 6.8: Reputation model behaviours when there is no trust loss

Model 6.7 is developed to calculate the reputation value of an owner when there is no trust gain τ_g value but trust loss τ_l value. In the model, we now have the data sensitivity

S_d value because when co-owners trust loss values are in the consideration which shows that co-owners have concerns on co-owned data security features. This refers to privacy loss model (see Equation 6.1).

$$
\begin{aligned}
c : \mathbb{R}, d : \mathbb{R} \\
Rep : cXd; \\
Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \\
c = 0, \\
d = \frac{-Sd * (1+\tau_l)}{2}, \\
Rep(0,d_i) = n * \frac{d}{d+2} \\
Rep(0,d) = \frac{\sum_{i=1}^{n} Rep(0,d_i)}{n}
\end{aligned}
\tag{6.7}
$$

Figure 6.9 indicates the changes on the reputation model with Equation 6.7. It is a function of the number of co-owners n for the data sensitivity value S_d. The data sensitivity value 0 is out of the calculation in the case. This is because if S_d is equal to 0, then it is impossible to have trust loss value since all co-owners are not worried about data security features. What is striking in Figure 6.9 is the rapid decrease on the reputation value when the data sensitivity value approaches 1.

The last case of changing reputation values of users is to have trust loss τ_l and trust gain τ_g values at the same time. This means that in data sharing process, some co-owners' trust in owner decreases while some co-owners' trust in owner increases. Equation 6.8 represents the reputation model when τ_l and τ_g both exist. The calculation of trust loss value for each co-owner is done with Equation 6.6 and the calculation of trust gain value

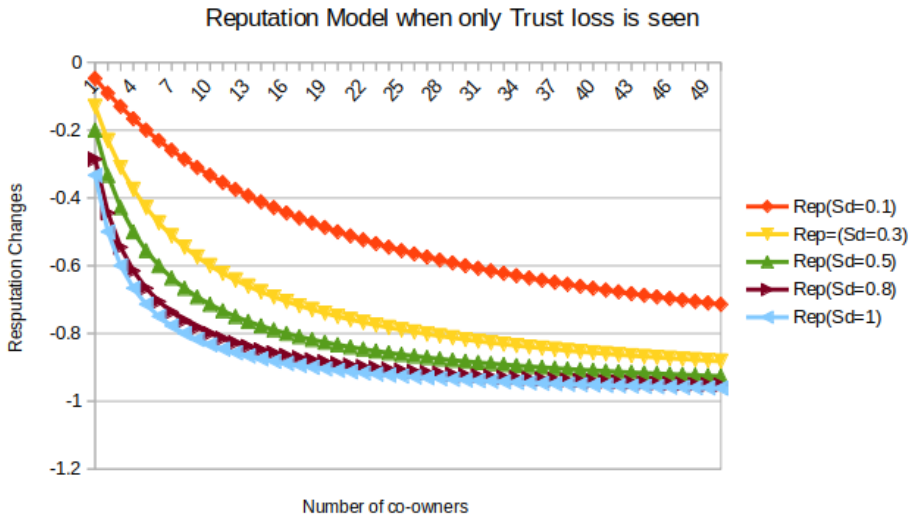

Figure 6.9: Reputation evaluation with varying the data sensitivity value when there is no trust gain value

for each co-owner is done with Equation 6.7.

$$
\begin{aligned}
c : \mathbb{R}, d : \mathbb{R} \\
Rep : cXd; \\
Rep : \mathbb{R}X\mathbb{R} \longrightarrow \mathbb{R} \\
c = \frac{Sd(1+\tau_g)}{2}, \\
d = \frac{Sd*(1+\tau_l)}{2}, \\
Rep(c,d) = \frac{(c-d)}{((c+d)+2)}
\end{aligned}
\tag{6.8}
$$

Figure 6.10 represents the changes on the reputation values with varying the trust loss and fastening the trust gain value to a certain value. In the figure *"Reputation Values when Trust Gain=0.1 by Changing Trust loss"*, the reputation decreases because trust loss value increases continuously. The figure reflects the expected behaviour of Model 6.8. The expectation is to see a decrease when trust loss value is greater than the trust

gain value. In the figure *"Reputation Values when Trust Gain=0.2 by Changing Trust loss"*, the reputation value starts with positive values. It then decreases this is because of the fact that the trust loss get greater values than trust gain value. Therefore, the reputation value takes negative values.

Figure 6.11, Figure 6.12, 6.13, and 6.14 represent also changes on the reputation model with different trust loss and trust gain values. The most important points in figures are that the reputation value is positive value when the trust gain value is greater than trust loss value.

6.3 Combining Co-owned Data Sharing Decision Cases with Reputation Changes

In this section, we show the combination of the reputation update cases with the decision cases. We have asked four questions in order to determine the cases. It is important to highlight that in this thesis the reputation values changes on a user's profile is done only if the content of data is co-owned.

Question	**Refers to**
What	It is asked to see Co-owners' consensus-reached group decision
How	It is asked to see Owner's final decision whether the owner respects the group's decision or not
with Whom	It is asked to see whether the targeted group for data is changed or not
with What	It is asked to see which permission is given to the targeted group

Table 6.2: Questions to Define Update Cases of a User's Reputation

Table 6.3 indicates the conditions and cases for defining whether owner's reputation value

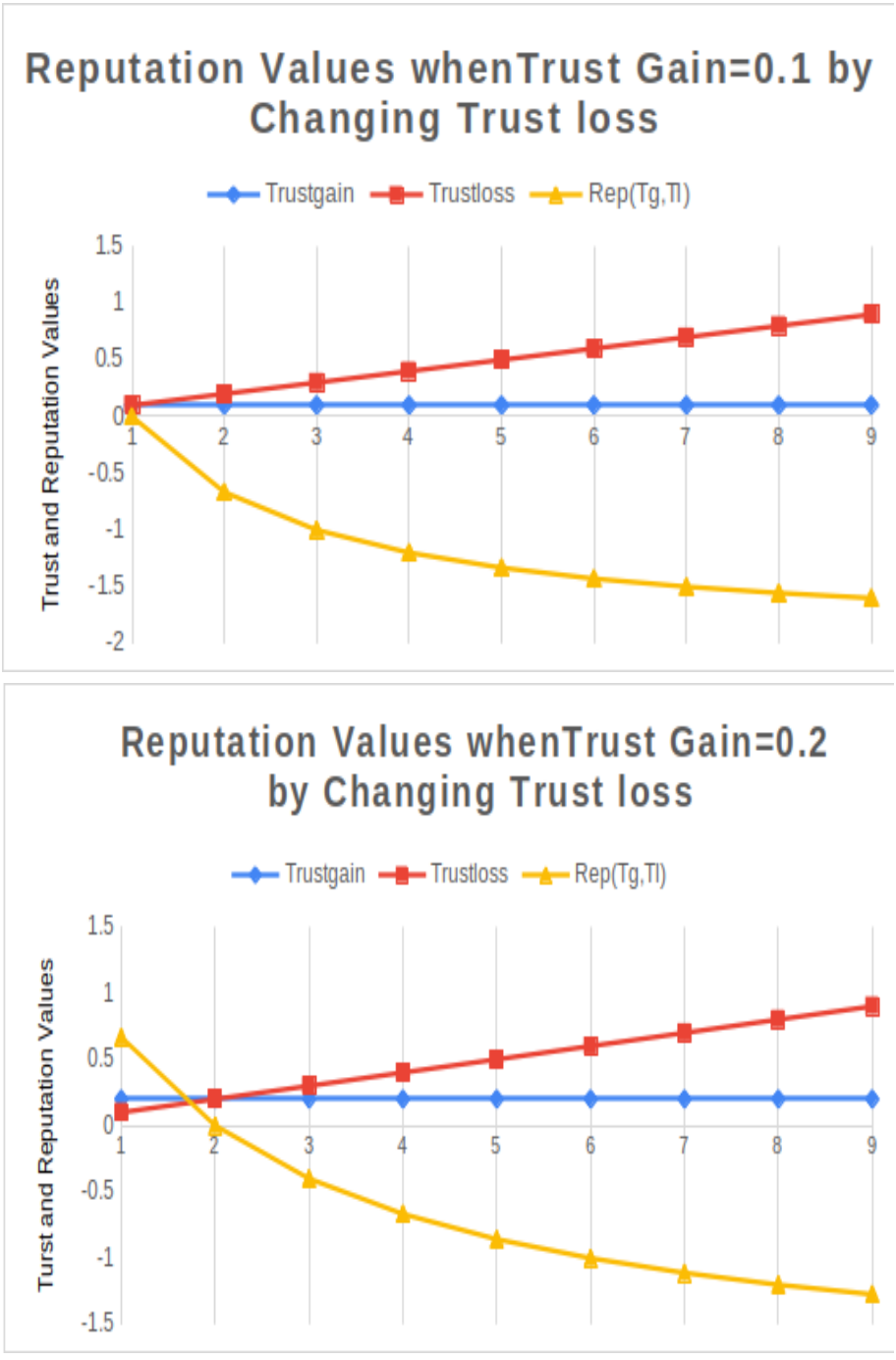

Figure 6.10: Changes on Reputation Values With Trust Gain Value And Trust Loss Value

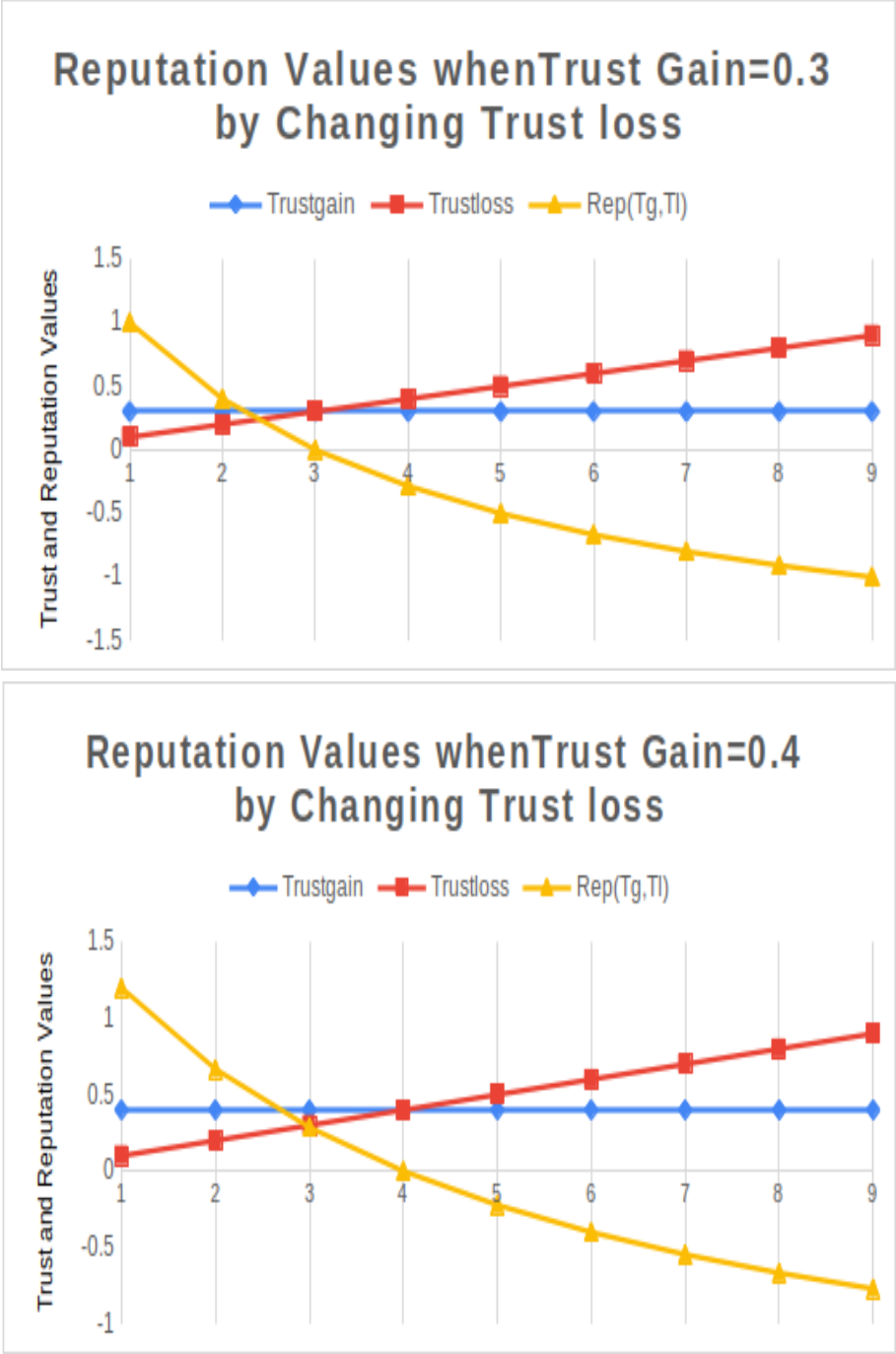

Figure 6.11: Changes on Reputation Values With Trust Gain Value And Trust Loss Value

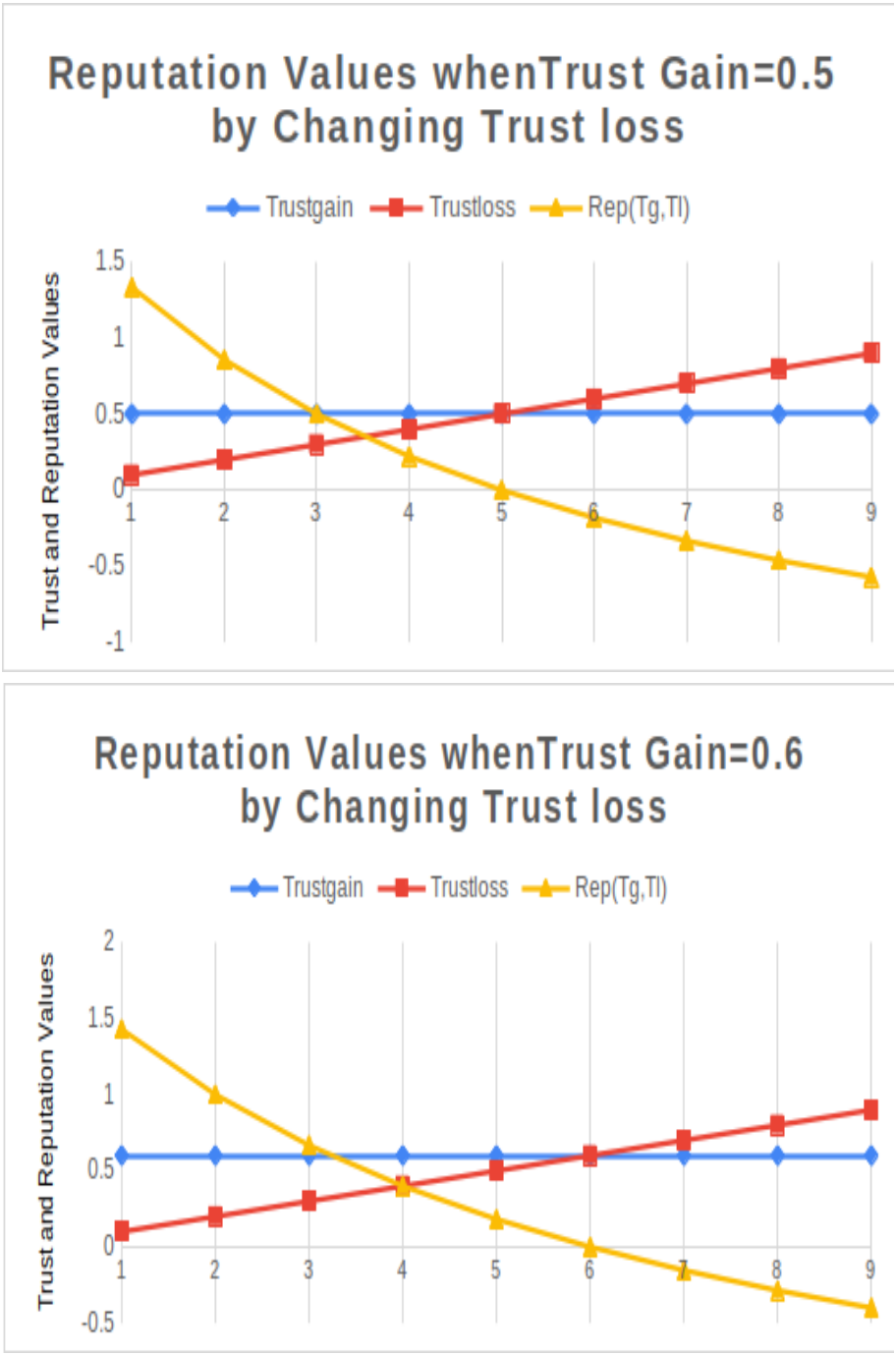

Figure 6.12: Changes on Reputation Values With Trust Gain Value And Trust Loss Value

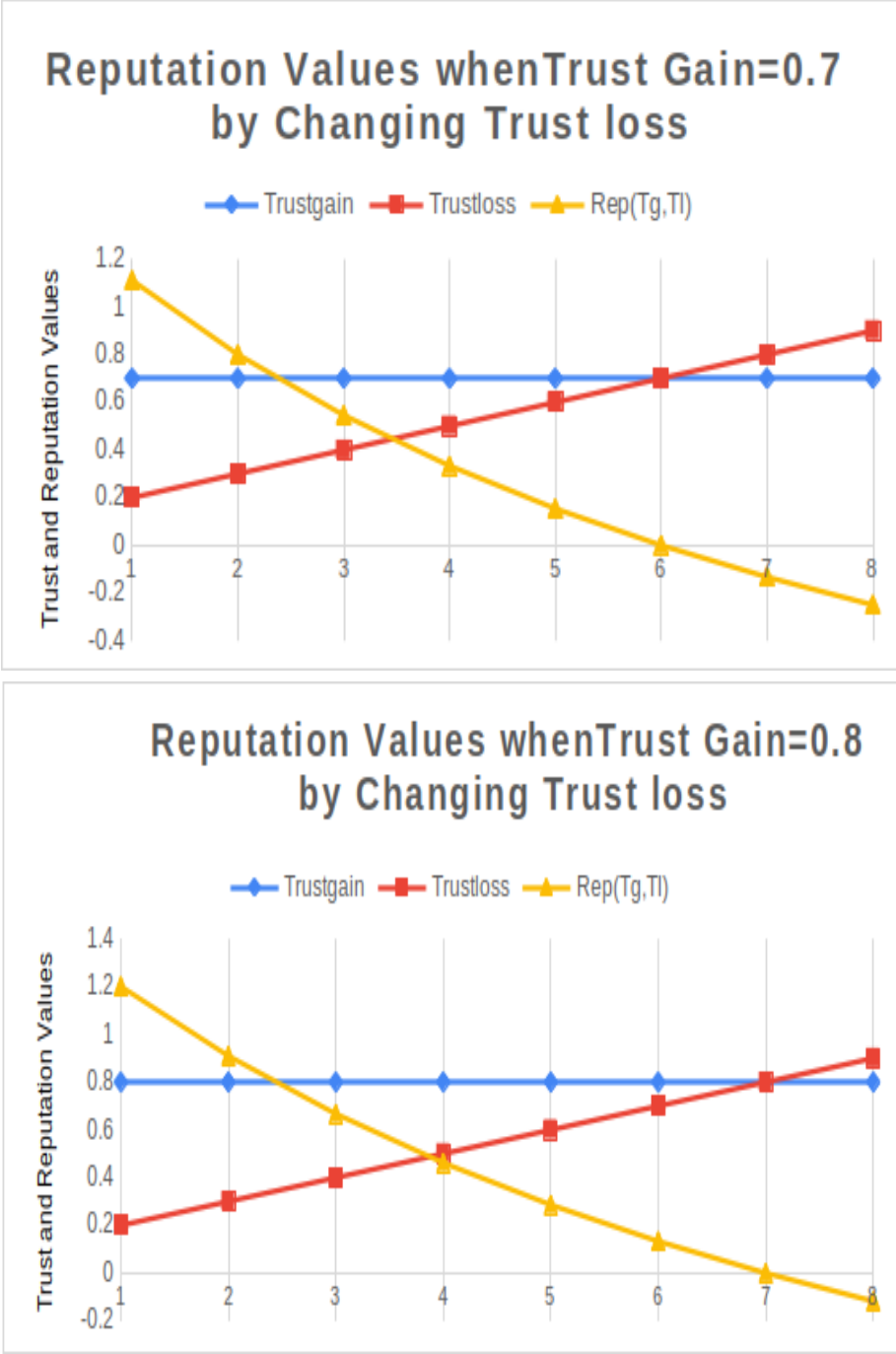

Figure 6.13: Changes on Reputation Values With Trust Gain Value And Trust Loss Value

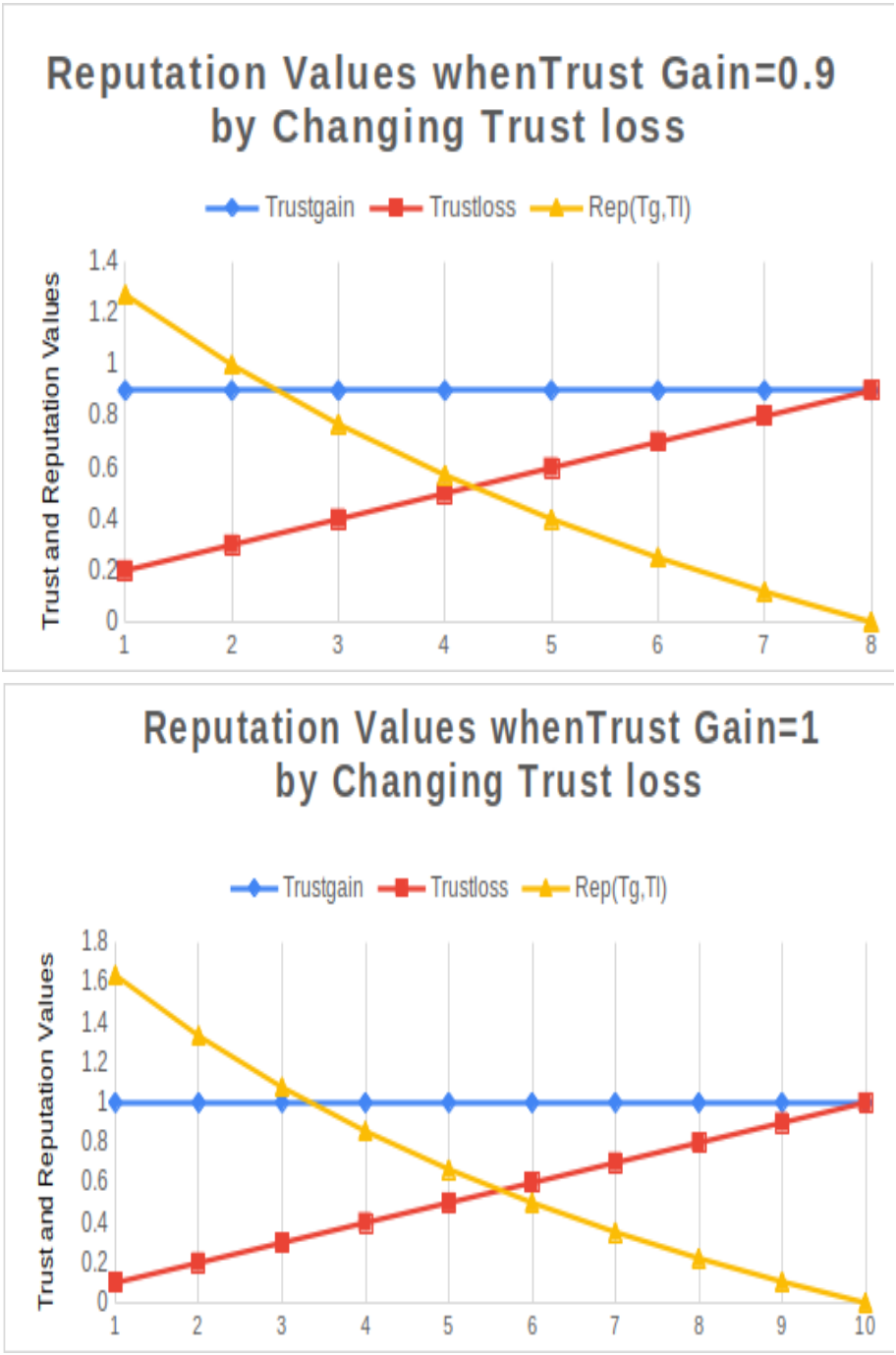

Figure 6.14: Changes on Reputation Values With Trust Gain Value And Trust Loss Value

Table 6.3: Reputation Update Rules

Co-owners' Decision	**Owner's Action**	**Reputation Changes** Rep_{ch}
YES ∧ Share with Full Permission	In any action	Changes the reputation Rep_{ch1}
YES ∧ Share with Restricted Permission	Share with Full Permission	Changes the reputation Rep_{ch2}
YES ∧ Share with No permission	Share with Full Permission ∨ Share with Restricted Permission	Changes the reputation Rep_{ch2}
Maybe ∧ Share with Full Permission	In any action	Changes the reputation Rep_{ch1}
Maybe ∧ Share with Restricted Permission	Permission	Changes the reputation Rep_{ch3}
Maybe ∧ Share with No Permission	Share with Full Permission ∨ Share with Restricted Permission	Changes the reputation Rep_{ch3}
No ∧ Not Share	Share with Full Permission ∨ Share with Restricted Permission ∨ Share with No Permission	Changes the reputation Rep_{ch2}
In all other cases	In all other cases	No changes

is updated. As it can be seen on the table, owner's reputation changes based on his action on the data sharing. If owner makes a decision to share the data that is congruent to co-owners' group decision, then the reputation value is increased. In contrast, if owner makes a decision to share the co-owned data that is against the co-owners' group decision, then the the owner' reputation value is decreased. In other cases and conditions, the reputation value remains same.

Each OSNs' member has a reputation value that is defined in below boxes. Updating conditions for a member's reputation are given on Table 6.3. In this thesis, we focus more on the reputation changes when the content of data is co-owned, therefore, the member whose reputation is updated, is the owner of the content. $Member \mapsto Rep$ represents that each member is assigned to a reputation value. The next box is used to update a member's reputation value which is presented as $Rep[[Member] \mapsto [Rep(member)+\delta(Rep_{ch}, c, d)]]$. As it is expressed before, we assume that each user is assigned a reputation value, therefore, the assigned reputation value is updated based on user's behaviours in a co-owned data sharing process only if the user takes the owner role in the sharing process. $\delta(Rep_{ch}, c, d)$ is the function which is used to update a member's reputation value. It has three different cases in this thesis (see equation 6.9). In Equation 6.9, conditions and cases in order to update a member's reputation in a co-owned data sharing process is covered. The first case is the one where all co-owners are happy to share the co-owned data and there is no trust-loss value for owner. If this is the case, then the function calls Equation 6.6 for updating the reputation value. When all co-owners are unhappy to share the co-owned data and the owner ignores co-owners' group decision, Equation 6.7 is called to update the owner's reputation value. In this case, the owner's reputation is decreased because of co-owner's concerns on co-owned data security features and permission on the co-owned data which might cause privacy leakage. The last case in the function happens when some

co-owners are happy and some are unhappy to share the co-owned data. Map: Member $\mapsto$ Rep Rep[[Member] $\mapsto$ [Rep(member)+$\delta(Rep_{ch},c,d)$]]

$$\delta(Rep_{ch},c,d) = \begin{cases} Rep(c,0), & when \\ & Rep_{ch}{=}Rep_{ch1} \\ Rep(0,d), & when \\ & Rep_{ch}{=}Rep_{ch2} \\ Rep(c,d), & when \\ & Rep_{ch}{=}Rep_{ch3} \end{cases} \tag{6.9}$$

6.4 Conclusion

This chapter gives trust and reputation models' developments and changes on the models. The trust loss and trust gain values are used to show co-owners' satisfaction and dissatisfaction in owner in a co-owned data sharing process in OSNs. Based on the owner's final decision in the co-owned data sharing process, the owner's reputation is updated. Losing trust in an owner means that the owner takes a decision which causes privacy concerns for a co-owner. Gaining trust means that the final decision in the sharing process does not cause any privacy concerns for a co-owner.

This chapter explains that having trust and reputation values in OSNs' platforms is an important need for OSNs' platforms. Having reputation values on OSNs' users' accounts can protect users from various threats in OSNs. We assume that the benefits of having the reputation values on users' accounts could be as follows;

- Realising the fake accounts: In OSNs, it is commonly seen that fake users imitate

the real users Ojo (2019); Hajdu et al. (2019); Yuan et al. (2019). A user can imitate another user by using the user's profile information including profile pictures. In such cases, other OSNs may not be able to recognise whether the account is fake or real. However, if the reputation values are used in OSNs' users' accounts, then it could be much easier to recognise whether an account is fake or real. Especially with the user whom OSNs' communicate with.

- Realising distressing OSNs' users: OSNs' platforms' users are free to post whatever content they want to post to either their own space or to other users spaces. These posts sometimes could involve unwanted contents such as hate speech Alkiviadou (2019); Carlson and Rousselle (2020). Some users get OSNs accounts just to motivate people for undesirable situations. Majority of OSNs use some techniques to remove hate speech from users' posts, however, users (*i.e. trouble makers*) can not be recognised by other users. In order to cope with those issues in OSNs, the proposed reputation models can be used. Because, even if a user removes his/her posts from OSNs, the reputation value is a persistent value and can lead the users to think whether that user is a good or a bad person.

Above points show that the reputation system is one of the most important part to make a balance between co-owned data sharing and users' privacy protection in co-owned data sharing processes. The reputation models here are the way to punish and award users based on their behaviours in a co-owned data sharing process. None of the previous work used such system to ensure users do not need to find a way to punish others if their privacy is leaked. It is the first time for using a reputation system in OSNs' data sharing process which shows how novel this thesis reputation system is.

This chapter presents the cases for updating an owner's reputation values based on the

owner's final decision in a co-owned data sharing processes in OSNs. This also means that this chapter explains one of the last steps to end a co-owned data sharing process in OSNs (see Figure 3.2 in Chapter 1).

Chapter 7

Formal Modelling of the Developed Framework

From Chapter 4 to Chapter 6, requirements, methods, equations, and models for completing a secure co-owned data sharing process in OSNs has been explained. Up until this chapter, the details of co-owned data sharing processes have been discussed. This includes co-owned data sensitivity value, confidence value in targeted group, co-owner's group's decision, and owner's decision, how is co-owned data shared/ which permission is given to the targeted group/ with whom co-owned data is shared, and the effect of completed data sharing process on users' reputation. This chapter aims to cover the explanation regarding how a shared co-owned data can be controlled with users' reputation values and the co-owned data sensitivity value. In OSNs, when a content of data is shared with a group of people, the control of data is transferred from the owner to the targeted group. The shared content of data can not be controlled when it is released to the targeted group due to the privacy settings in OSNs Lu and Li (2020). This is because the shared content might flow to users who are not supposed to access the shared content. Control-

ling the shared content has recently been taken into consideration by OSNs platforms. For example, Facebook has recently started control shared contents of data, however, the attempted step restricts permissions to the first targeted group and does not allow first targeted group's members to re-share data Quora (2019). Therefore, it is a need to define a formal way which should be able control a shared co-owned data with more specifications in OSNs platforms. With this respect and with the developed framework in this thesis, this chapter presents a formal way to control shared co-owned data in OSNs. Because formal modelling helps to see what is missing in a system therefore any system before its implementation should be modelled with a formal language. This chapter analyses not only the usability of the developed framework but also missing points if there is any.

In order to analyse the developed framework in a system level, Event-B is used. Event-B Joseph (2014) is used to control the flow of co-owned data after it is shared. Event-B is a formal method for system-level modelling and analysis. Key features of Event-B are the use of set theory as a modelling notation, the use of refinement to represent systems at different abstraction levels and the use of mathematical proof to verify consistency between refinement levels. As it can be seen up until this chapter includes a theoretical framework and mathematical equations in it which are required a system level analysis. The aim is to keep high sensitive co-owned data in a secure sharing track. This means that high sensitive data should not be shared with low reputed users. Event-B Abrial (2010) is also used for formal modelling of the flow control because it is used to model and analyse systems. It is also used to model and develop systems based on the conditions. The key features of Event-B are the use of set theory as a modelling notation, the use of refinement to represent systems at different abstraction levels and the use of mathematical proof to verify consistency between refinement levels.

7.1 An overview on Event-B Syntax

The aim of this section is to give an overview explanation on Event-B language syntax, following explanations are given with the use of the work in Abrial et al. (2005) as base. In Event-B, there are two basic constructs *context* and *machine*. The static part of a model in Event-B is defined in the *context* part. And the the dynamic part of a model in Event-B is defined in *machine* part. Machines and contexts have different relationships: a machine can see one or various contexts for a model. A machine can be refined by another machine. Moreover, a context can be extended by another one.

Carrier sets, *constants*, *axioms*, and *theorems* are defined in *context* section in an Event-B. A *machine M* contains *variables*, *invariants*, *theorems*, *events*, and *variants*. Variables v define the state of a *machine* in Event-B. Variables are constrained by invariants $I(v)$. Any changes in states are described in events.

Each event composes of a *guard G* and an *action S*, where the guard necessary states for an event and the action describes how the variable evolve when an event occurs. An event might have local variables. In such cases the representation of *guard* and *action* for the event being occurred are as; *guard* $G(t,v)$ and an action *action* $S(t,v)$ where t indicates the local variable and v stands for the variables defined in $I(v)$. An event E can be specified with three following forms;

$E \triangleq$ **begin any** t **where** $G(t,v)$ **then** $S(t,v)$ **end**

$E \triangleq$ **begin when** $G(v)$ **then** $S(v)$ **end**

$E \triangleq$ **begin** $S(v)$ **end** Event-B has simple mathematical language, such as integers or given sets that are specific to a model or are formed from the Cartesian product and power-set type constructors. The definition of relations and functions is done by combining those constructors. Event-B language is designed with basic mathematical concepts therefore

set theory and logic are used for descriptions as same as any engineering disciplines. Event-B notations therefore are defined in the same way of the mathematics notations. Table 7.1 gives some of the maths notations, Event-B notations, and definitions.

Maths Notation	Event-B Notation	Definition
$\in$	:	set membership
$\mathbb{N}$	NAT	natural numbers
$\leq$	$<=$	less than or equal
T	true	Boolean true
$\bot$	false	Boolean false
$\subseteq$	$<:$	subset or equal
$\subset$	$<<:$	strict subset not equal
$\rightarrow$	$-->$	denotes a total function
$+->$	$+->$	denotes a partial function
$\varnothing$	$\{\}$	empty set
$\neq$	$/=$	not equal
$\mapsto$	$\|->$	maps to

Table 7.1: Mathematical Notation and Event-B Notation

7.2 Shared Contents of Co-owned Data Flow Control

Each data needs be owned by a user in order to upload, create, use or share, not only in the real life communications, but also in communication of OSNs. A user might be the owner, co-owner, or accessor (*i.e. viewer*) for co-owned data in OSNs. Each role should have different permissions and/or actions in co-owned data sharing processes in OSNs. Therefore, define roles and activities have been defined considering that which roles can be given to a user and which activities are related to which roles. Figure 7.1 presents the structure of activities with their associated roles. As it is seen in the figure, a user, who has owner role, has three activities, a user, who has co-owner role, has one activity, and a user, whose role is viewer, has two activities in a content of co-owned data sharing process. The owner role's activities and co-owner role's activities are given in the

previous chapters. This research focuses more on the viewer role in this chapter because the aim is to control shared a co-owned content. This means that the control starts after the content is accessed by a viewer.

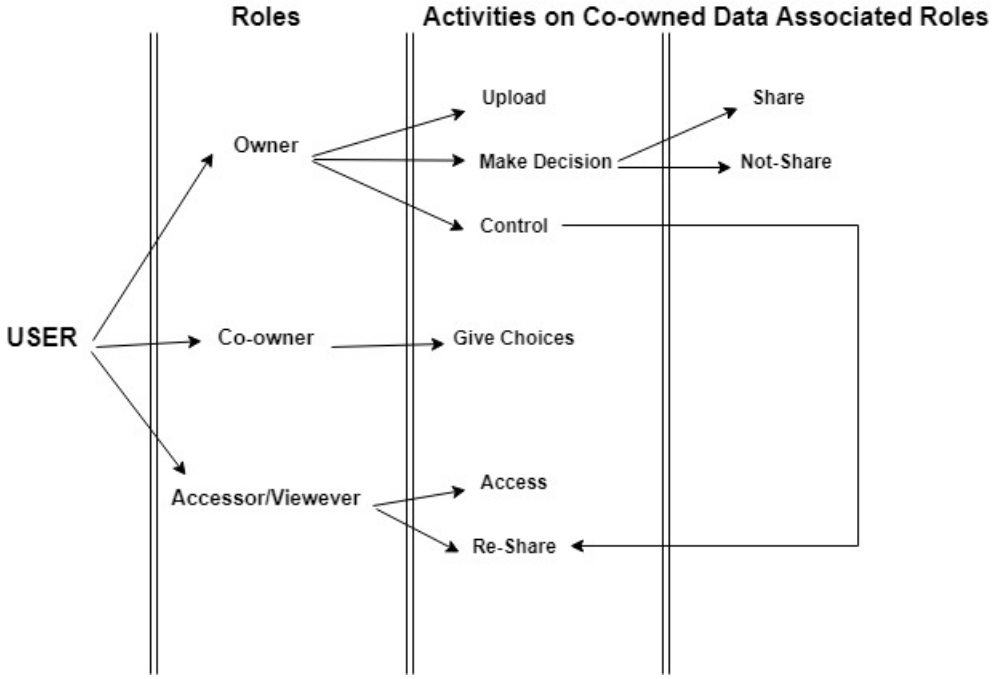

Figure 7.1: Activities on Co-owned Data Associated with a User's Role

$USERS=\{u_1, u_2, u_3,.....,u_k\}$, be a users set. The users are one of the main factors in OSNs since the main purpose of OSNs is to encourage users to be member in OSNs. Users are people who use OSNs for any purpose, however, a user might have different roles in different data sharing processes in OSNs. For instance, a user might be the owner of a content of data in OSNs, a viewer for another content of data, or a co-owner for the content of data. The term user covers all above mentioned cases.

$DATA=\{d_1, d_2, d_3,....., d_l\}$ be the set of contents of data shared in OSNs. The content of data can either be owned by only one user (i.e. *single-owned data*) or by several users (i.e. *co-owned data*). Here, owning refers to the number of users' id on the content of data. If a content is owned by at least two users, then the content is called co-owned data.

ROLES={*owner, co-owner, viewer/ accessor*} be set of roles associated to users in the data sharing process. In OSNs, a user might become an owner for a shared content while he was a viewer for the same content before. In such a case, the content might be revealed to users who were not allowed by the first owner of the content. In order to cover this gap, we introduce a new activity *control*, where the first owner can specify following viewers/ accessors for the shared content. In this way, controlling the shared contents can be done in OSNs which is a way to preserve co-owners' privacy for the future flow of co-owned data.

ACTIVITIES={*upload, take-decision, share/ not share, give-choices, access, re-share, control re-share*} be the set of activities in OSNs related the roles associated to users in a data sharing process. In Figure 7.1, relationships between activities and roles have been given. In this chapter, the focus is on the association between activity re-share with the accessor/ viewer role and the control with owner role.

PERMISSIONS(Re-Share)=allow and deny be a set of permissions that demonstrates the first user, who shares the content of data, decided whether to control the flow of shared data or not. Re-share refers to the permission given to the first targeted group' members by the owner. The flow of shared data can be controlled with specifying permissions in the beginning of a data sharing sequence in OSNs. To do so, OSNs need more consideration on functions (*i.e. events*).

REPUTATION: be a set of integer numbers. In Chapter 6, we have given the models for users' reputation in OSNs. We now assume that each user is given a reputation value in OSNs. It is aforementioned that the reputation value is a dynamic value. It changes with respect to users' behaviours in a co-owned data sharing process. As it has been explained in Chapter 6, it increases if a user behaves in a good way, i.e. respecting co-owners decisions. Sharing a co-owned content causes increment on the reputation value. Bad

behaviour causes decrease in reputation value.

$$\begin{aligned} reputed[u] &= i \\ where, & \\ i &\in \mathbb{R} \\ reputation[i] &\in [0,...,\mathbb{R}] \end{aligned} \tag{7.1}$$

DATA SENSITIVITY: be a set of integer numbers where the numbers range from 0 to 10. In Chapter 1, we have explained the model for the data sensitivity value and the co-owned data sensitivity value ranges in [0,...,1].

$$\begin{aligned} has[d] &= l \\ where, & \\ l &\in \mathbb{R} \\ has[l] &\in [0,...,1] \end{aligned} \tag{7.2}$$

7.3 Formal Modelling

This section presents mathematical concepts of the developed framework. The use of mathematics here helps us to ensure the construction of correct flow control of co-owned data in OSNs since it is precise and unambiguous, unlike natural language. It forces us to think deeply about the system's behaviour, and allows formal analysis.

Definition 7.1. ***Assigns to****: The developed framework assigns roles to users, sensitivity value to co-owned data, and reputation values to users.*

- $reputed \in USERS \longrightarrow \mathbb{Z}$

*It is a **total function** that relates each element of the source with exactly one element of the target. Each user in the system has only one reputation value. None of the users should be assigned more than one reputation value. However, one reputation value can be given to more than one user in the system.*

reputed(u,r) means that user u is assigned to the reputation value r.

$\forall\, u.(u \in USERS \wedge r \in \mathbb{R}) \implies reputed(u,r)$

- $has \in co\text{-}owned \longrightarrow \mathbb{Z}$

  *It is a **total function** that relates each element of the source with exactly one element of the target. Each co-owned data in the system has only one data sensitivity value. None of the co-owned data should be assigned to more than one sensitivity value. However, one sensitivity value can be given to more than one co-owned data in the system.*

  has(d,l) means that co-owned data d is assigned to the sensitivity value l

  $\forall\, d.(d \in co\text{-}owned \wedge l \in [0,...,1]) \implies has(d,l)$

- $access \in targetedgroup \longleftrightarrow co\text{-}owned$

  Let targetedgroup be a subset of USERS which involves users who are chosen for being an accessor/viewer for co-owned data. It is the set of relations between users and co-owned data in the system. It means that the users in targeted group set can access to co-owned data.

  $\forall\, u.(u \in targetedgroup \wedge d \in co\text{-}owned \implies access(u,d)$

Definition 7.2. ***Re-sharing:*** *Each shared co-owned data, which is held by the targeted group, might be shared with a new group of people or person. Figure 7.2 illustrates the general structure of co-owned data sharing process and introduces notions and the requirements of the system. In the figure, Re-Share event happens only if co-owned data are accessed by the targeted group. The first condition is on Re-share and it is defined as*

follows;

$\forall\, d.\ (d \in \textit{co-owned}) \wedge \forall\, u.\ (u \in \textit{targetedgroup}) \wedge \textit{access}\ (u,d) \implies \textit{Re-share}(u,d) \wedge \forall\, u.\ (u \in \textit{USERS})$

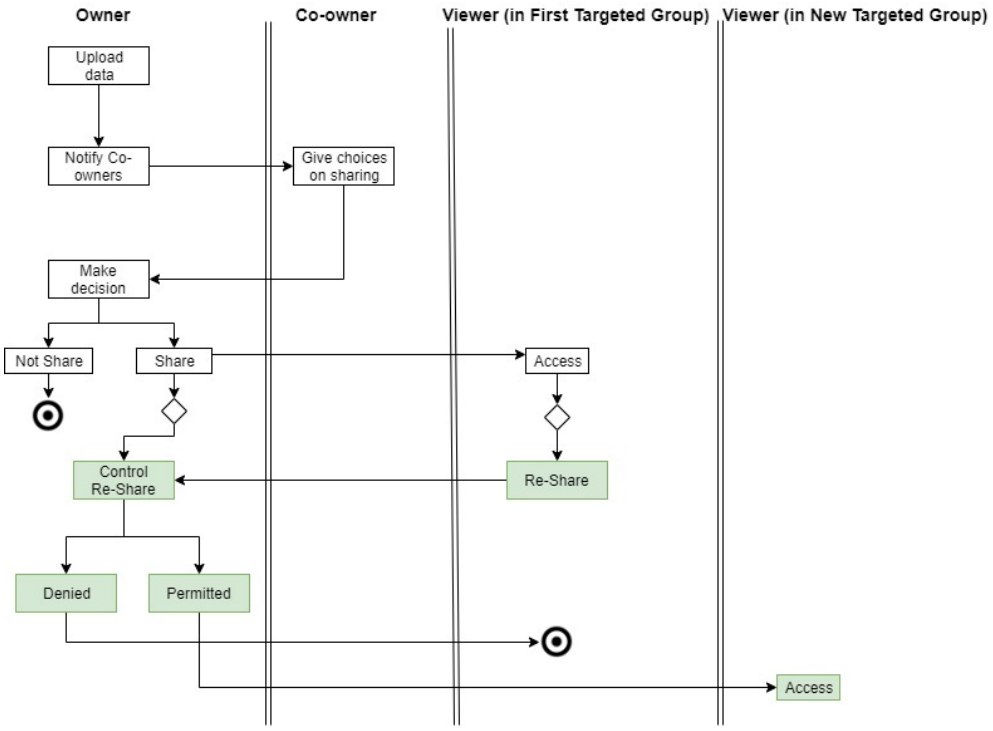

Figure 7.2: Data Sharing Process Diagram

Definition 7.3. ***Control Re-sharing and Conditions:*** *Any shared co-owned data requires re-sharing specifications on controlling or not controlling the flow of co-owned data for the next targeted group. This means that the data owner can either choose to control or not to control the flow of shared co-owned data in OSNs. The control flow is done only if the data owner wants to control the flow of shared co-owned data. With the developed framework, OSN platform needs to control the flow of shared co-owned data. The main purpose here is to ensure that the high sensitive co-owned data is in the circle of trusted people who are not expected to cause any privacy issues with re-sharing the high sensitive co-owned data.*

$\forall$ *d (access(u,d)* $\wedge$ *Re-share(u,d))* $\Longrightarrow$ *Control Re-share(reputed(u,r), has(d,l))*

Flow of co-owned data is controlled when Re-Share happens. Control Re-share(reputed(u,r), has(d,l)) is an activity/ event where users' reputation and co-owned data sensitivity are used as check points. These check points have conditions, which are as follows;

- *high co-owned data should not be flown to users whose reputation is not high. This ensures that high sensitive shared co-owned data will never been accessed by users who have leaked users' privacy in the past co-owned data sharing processes. Definition 7.4 gives the formal modelling and its conditions on co-owned data sensitivity class and users' reputation class. The system will never allow high sensitive data flow to users whose reputation class is not high.*

  Definition 7.4. $\forall$ *d,u. (d,u* $\in$ *Control Re-share(reputed(u,r), has(d,l))* $\wedge$
  $\forall$ *d. (d* $\in$ *has(d,l)* $\wedge$ *(value[l]* $\in$ *high)* $\wedge$ $\forall$ *u. (u* $\in$ *reputed(u,r)* $\wedge$ *(value[r]* $\in$ *high)*
  $\Longrightarrow$ *access(u,d)*

- *Another restriction is on medium sensitive co-owned data (Note: the classes of co-owned data sensitivity are high, medium, and low (Chapter 5)). Medium sensitive co-owned data might also cause security issues if it is shared with users, whose reputation values are low. Therefore, the system should never allow medium sensitive data flow to low reputed users.*

  Definition 7.5. $\forall$ *d,u. (d,u* $\in$ *Control Re-share(reputed(u,r), has(d,l))* $\wedge$
  $\forall$ *d. (d* $\in$ *has(d,l)* $\wedge$ *(value[l]* $\in$ *medium)* $\wedge$ $\forall$ *u. (u* $\in$ *reputed(u,r)* $\wedge$ *(value[r]* $\geq$
  medium) $\Longrightarrow$ *access(u,d)*

In Definition 7.4 and Definition 7.5, conditions are on co-owned data sensitivity and users' reputation values. Definition 7.4 checks if co-owned data belongs to high sensitive class

and users' reputation is high who are targeted for high sensitive co-owned data, then access permission is allowed for those users. Definition 7.5 checks if co-owned data belongs to the medium sensitive class and users' reputation values are at least medium and high, then access permission is allowed for those users.

7.3.1 Variables' Normalisation

In the formal modelling and analysis of a system, it is important to know how the system needs to behave under which circumstances. With this respect, this section of the chapter specifies the requirements and the functions. In Chapter 7 and Chapter 5, the reputation and the co-owned data sensitivity values are the real numbers, however, we use integer numbers in this section. The reason being we use *Event B* tool in order to prove defined formal models and *Event B* tool does not provide the real numbers' usage, therefore, we convert real numbers to integers.

The first integer, commonly known as the significant, is to be interpreted as a float with the floating point occurring after the first two decimal digits. The second integer is to be interpreted as the power of 10, commonly known as the base, which is to be multiplied to the significant in order to give the real value of the floating point number (significant x 10^{base}) Gibson and Méry (2018). In order to do conversion and not missing any values in the system, we multiply the reputation values and the sensitivity value with base two.
Normalisation factor[reputation] = (significant x 10^2) $\implies$ n *where* n $\in [0-\mathbb{Z}]$.

Normalisation factor[sensitivity] = (significant x 10^2) $\implies$ n *where* n $\in [0-10]$.

We give the conversion of real numbers into the integer numbers with the dimensions and the application of normalisation factors for all units in the data sensitivity and the reputation values.

Table 7.2 explains mapped values of the reputation values and the co-owned data sensitivity values after applying the normalisation on those values.

Table 7.2: Values as Reel Numbers

Elements of X_i Set	**Definition**	**class**
reputation	$\forall_r.\mathrm{r} \in \mathbb{Z}$	_
sensitivity	$\forall_l.\mathrm{l} \in \mathbb{Z}$	_
reputation	$\mathrm{r} \mid \mathrm{r} \in \mathbb{Z} \wedge \mathrm{r} \in [0\text{-}130)$	Low
reputation	$\mathrm{r} \mid \mathrm{r} \in \mathbb{Z} \wedge \mathrm{r} \in [130\text{-}290)$	Medium
reputation	$\mathrm{r} \mid \mathrm{r} \in \mathbb{Z} \wedge \mathrm{r} \in [290\text{-}400]$	High
sensitivity	$\mathrm{l} \mid \mathrm{l} \in \mathbb{Z} \wedge \mathrm{l} \in [0\text{-}40)$	Low
sensitivity	$\mathrm{l} \mid \mathrm{l} \in \mathbb{Z} \wedge \mathrm{l} \in [40\text{-}70)$	Medium
sensitivity	$\mathrm{l} \mid \mathrm{l} \in \mathbb{Z} \wedge \mathrm{l} \in [70\text{-}100]$	High

7.4 Context and Machines of Controlling Co-owned Data Flow Point in Developed Framework

Context machine presents the sets, constants, and axioms of the system. *USERS, DATA*, and *permission* are the sets that are used in the whole system. *Constants* define the variables whose values remain same during the system development. In our case, *users, targetedgroup, yes*, and *no* are the variables whose values are stable. *targetedgroup* represents the first targeted group of people for co-owned data and *users* indicates any user in OSN platform.

CONTEXT

CoownedDataC

SETS

USERS

DATA

permission

CONSTANTS

users

targetedgroup

yes

no

AXIOMS

axm1: USERS$\neq\varnothing$

axm2: DATA $\neq\varnothing$

axm3: users$\subseteq$USERS

axm4: targetedgroup$\subseteq$USERS

axm5: permission= {yes,no}

axm6: yes$\neq$no

END

Machine *CoownedDataM* introduces the abstract machine which uses the sets. The names of variables, whose values comprise the machine, state the machine declared within the *variables* clause. The *invariant* provides information concerning state (i.e. variables) of the machine, including the types of variables and restrictions on their values for the state to be considered meaningful.

CoownedDataM machine represents an OSN platform which uses the developed framework with users' reputation values and co-owned data sensitivity value for controlling shared co-owned data flow. The machine sees *CoownedDataC*, variables are *reputed, coowned, has*, and *access*. Details of each invariant are as follows;

- $reputed \in USERS \implies \mathbb{Z}$

Each user in the members set has a reputation value which is named reputed and it is assigned to a numerical value in $\mathbb{Z}$. A user can only have one reputation value but one reputation value can be given to more than one user.

- $has \in coowned \implies \mathbb{Z}$

  Each coowned data has only one value in $\mathbb{Z}$ but one data sensitivity value can be assigned to more than one data.

- $coowned \subset DATA$

  Each data which is an element of coowned set is also an element of *DATA*. This is needed because every data in co-owned set needs to have a sensitivity value.

- $access \in targetedgroup \longleftrightarrow coowned$

  Each member in the first targeted group set has an access data in co-owned set. This is an interesting invariant because the system's controlling point starts from this invariant. When a user in targeted group has access to co-owned data, the user can re-share the data. However, this work introduces that the system has control points for co-owned data flow.

The abstract machine is responsible for assigning users' reputation, co-owned data sensitivity value, and allows first targeted group for accessing co-owned data. There are three events in the machine, *assignusersreputation(u,r)*, *assigncoowneddatasensitivity(d,l)*, and *accessfirsttargetedgroupcoowneddata(u,d)* respectively. The machine's behaviours on the given events is as follows;

MACHINE

CoownedDataM

SEES

CoownedDataC

VARIABLES

reputed

co-owned

has

access

INVARIANTS

userreputation: reputed$\in$USERS$\rightarrow\mathbb{Z}$

coowneddata: coowned $\subset$DATA

coowneddatasensitivity: has$\in$coowned$\rightarrow\mathbb{Z}$

accessrelation: access$\in$targetedgroup$\leftrightarrow$coowned

EVENTS

assignusersreputation$\triangleq$

STATUS

ordinary

ANY

u

r

WHERE

grd1: u $\in$ USERS

grd2:r $\in \mathbb{Z}$

THEN

act1: reputed(u) := r

END

assigncoowneddatasensitivity$\triangleq$

STATUS

ordinary

ANY

d

l

WHERE

grd1: d ∈ DATA

grd2:l ∈ ℤ

grd3: d∉ coowned

THEN

act1: coowned= coowned ∪ {d}

has(d)=l

END assignfirsttargetedgrouptocoowneddata≙

STATUS

ordinary

ANY

u

d

WHERE

grd1: u ∈ targeetdgroup

grd2:d ∈ coowned

THEN

act1:access=access ∪ {u↦d}

END

END

- Event *assignusersreputation(u,r)*: The event takes two variables *u,r* as guards, these are necessary conditions for the event to occur. This event picks any user *u* from

the USERS set and assigns a reputation value r to the user u, where $r \in \mathbb{Z}$.

- Event *assigncoowneddatasensitivity(d,l)*: This events takes *d,l* variables as guards. The data *d* is the member of DATA but not a member in the coowned set. This event adds the *d* to the coowned set and assigns an integer value to data as a value which indicates the sensitivity value for the data.

- The next event is *accessfirsttargetedgroupcoowneddata(u,d)*: It is an event that allows access user *u* to data *d*. As it is aforementioned that this is first condition for controlling co-owned flow data because the targeted group's users needs to have access and start dissemination of co-owned data.

7.4.1 Refinement

Given machine shows what behaviour is required for an implementation. Now, we explain how the given behaviour should be achieved (see *CoownedDataMR*). Refinement machine includes aspects of how the behaviours are to be achieved in the implementation. The refined machine represents the addition of more detail to the initial abstract machine. The refined machine is now able to control the flow of shared coowned data based on the conditions on shared coowned data sensitivity values and users' reputation values. The refined machine's invariants have more specified conditions for making sure that the sensitive data does not flow to unwanted members in the system. The refinements on the variables, invariants, and events are as follows;

- ***reshare*, *controlledaccess*, *reshareddata*, and *permitted* (variables)**: Given variables are the new variables in the refined machine. We now explain given variables' detailed definition with related invariants.

- **resharedtargetedgroup:** $reshare \in targetedgroup \rightarrow coowned$;

  This invariant introduces total function *reshare* from *targetedgroup* set to *coowned* set. Any user in the targeted group can reshare co-owned data which was accessed by him. Access has been defined in the abstract machine.

- **reshareddatafromcoowned:** $reshareddata \subseteq coowned$:

  Any data in *reshareddata* set has to be an element of *coowned* set.

- **permittedordenied:** $permitted \in permission$

  It is a new invariant which can have only two values either *yes* or *no*, which are constants of permission set in the context machine.

- **controlledaccessisusertoreshared:** $controlledaccess \in reshareddata \rightarrow permission$

  It is a checkpoint of re-shared co-owned data which shows whether the permission is allowed (i.e.*yes*) or denied (i.e.*no*).

- **resharingcontrol:** It introduces the condition on the re-shared co-owned data with;

  $\forall\, d.\ (d \in reshareddata) \wedge (\forall.\ (u \in users)) \wedge d \in ran(access) \implies permitted{=}yes$

  Any user *u* in *users* set is permitted to any data *d* in *reshareddata* set where the data *d* has to be an element of *coowned* set.

- **resharingaccesscontrolpoint1:** It is a refinement on event *accessfirsttargetedgroupcoowneddata* in the abstract machine. As it is aforementioned that all refinements are on event *accessfirsttargetedgroupcoowneddata* because of the starting point of dissemination of co-owned data. In order to access re-shared co-owned data, the system should go over various guards. The details of each guard's is as follows;

  - $u \in users$: User *u* in the users set.

- $d \in coowned$ and $d \notin reshareddata$: Data has to be accessed by co-owners and then it can be re-shared. Therefore data d is an element of *coowned* set but not an element of *reshareddata* set.
- *permitted=no*: At the beginning, the data is not permitted for dissemination.
- Conditions are on the data sensitivity and the users' reputation values. Therefore, it is important to check users' reputation values with $r \in \mathbb{Z} \wedge 290 < r \leq 400$, which ensures that the user u' reputation r is in high class and co-owned data sensitivity value with $l \in \mathbb{Z} \wedge 70 < l \leq 100$ is high sensitive (see Definition 7.4).

When all guards are correct, the event *act1* and *act2* occur.
reshareddata:= reshareddata $\cup$ *d*: Data *d* is moved to reshared data and
controlledaccess:= controlledaccess $\triangleleft \forall$ *u. (u* $\in$ *users)* $\wedge$ *reputed(u):=r* $\wedge \forall$*d. (d* $\in$ *reshareddata)* $\wedge$ *has(d):=l* $\implies$ *permitted=yes*: All users whose reputation values are in the range of guard (*grd7*), are permitted to access the re-shared co-owned data which has high sensitivity (*grd6*).

- **resharingaccesscontrolpoint2:** It is the second refinement on event *accessfirsttargetedgroupcoowneddata* in the abstract machine. The details of each guard's in the event are as follows;
  - $u \in users$: User u in the users set.
  - $d \in coowned$ and $d \notin reshareddata$: Data has be to be accessed by co-owners and then it can be re-shared. Therefore, data d is an element of *coowned* set but not an element of *reshareddata* set.
  - *permitted=no* At the beginning, the data is not permitted for dissemination.

– Conditions are on the data sensitivity value and the users' reputation values. Therefore, it is important to check users' reputation values with $r \in \mathbb{Z} \wedge 130 < r \leq 290$, which ensures that the user u' reputation r is in at least medium class and co-owned data sensitivity value with $l \in \mathbb{Z} \wedge 40 < l \leq 70$ is medium sensitive (see Definition 7.5).

When all guards are correct, the event *act1* and *act2* occur.

reshareddata:= reshareddata $\cup$ *d*: Data *d* is moved to reshared data and

controlledaccess:= controlledaccess $\triangleleft \forall$ *u. (u* $\in$ *users)* $\wedge$ *reputed(u):=r* $\wedge \forall$*d. (d* $\in$ *reshareddata)* $\wedge$ *has(d):=l* $\Longrightarrow$ *permitted=yes*: All users whose reputation values are in the range of guard (*grd6*), are permitted to access the re-shared co-owned data which has high sensitivity (*grd5*).

MACHINE

CoownedDataMR

REFINES

CoownedDataM

VARIABLES

reshare

Controlledaccess

reshareddata

permitted

INVARIANTS

resharestargetedgroup: reshare $\in$ targetedgroup $\rightarrow$Coowned

reshareddatafromCoowned:reshareddata $\subseteq$Coowned

permittedordenied:permitted $\in$permission

Controlledaccessisusertoreshared: Controledaccess $\in$ reshareddata $\rightarrow$ permission

resahringcontrol: $\forall$d. (d$\in$reshareddata) $\wedge$ $\forall$u.(u $\in$users) $\wedge$ d $\in$ ran(access) $\implies$ permitted=yes

EVENTS

resharingaccesscontrolpoint1 $\triangleq$

STATUS

ordinary

REFINES

accessfirsttargetedgrouptocoowneddata

ANY

u

d

WHERE

grd1:u $\in$ users

grd2: d $\notin$ reshareddata

grd3: d $\in$ coowned

grd4:permitted=no

grd5:l $\in \mathbb{Z} \wedge (70<l\leq 100)$

grd6:r $\in \mathbb{Z} \wedge (290 < r \leq 400)$

THEN

act1: reshareddata := reshareddata $\cup \{d\}$

act2: Controlledaccess= Controlledaccess $\lhd\!\!+$ ($\forall$u. (u $\in$ users $\wedge$ reputed(u)=r) $\wedge$ ($\forall$d. (d $\in$ reshareddata $\wedge$ has(d)=l) $\implies$ permitted=yes)

END

resharingaccesscontrolpoint2 $\triangleq$

STATUS

ordinary

REFINES

accessfirsttargetedgrouptocoowneddata

ANY

u

d

WHERE

grd1:u $\in$ users

grd2: d $\notin$ reshareddata

grd3: d $\in$ coowned

grd4:permitted=no

grd5:l $\in \mathbb{Z} \wedge (40 < l \leq 70)$

grd6:r $\in \mathbb{Z} \wedge (130 < r \leq 290)$

THEN

act1: reshareddata := reshareddata $\cup \{d\}$

act2: Controlledaccess= Controlledaccess $\lhd\!\!+$ ($\forall$u. (u $\in$ users $\wedge$ reputed(u)=r) $\wedge$ ($\forall$d. (d $\in$ reshareddata $\wedge$ has(d)=l) $\implies$ permitted=yes)

END

7.5 Summary

In this chapter, we have presented a formal specification and formal modelling regarding the future flow of shared coowned data in OSNs' platforms. We have first started with the diagram of the proposed work, which covers users' and data interactions with the specifications of activities. The proposed work formal modelling requires definition of the sets, relationships between sets, and roles of the each attributes in the system as a second step. It is needed to give the most important part of the system with co-owned

data sharing process diagram to highlight the most focused activities. We have shown the needs of highlighting in Figure 7.2. Green boxes present the control flow of co-owned data in the developed framework. The focused part of Figure 7.2 is formalised. Using the defined requirements, functions, relations and sets, we have created a machine in Event-B defines the control future flow of co-owned data in the system.

The abstract machine is the first level which does not specify the conditions for re-sharing action in the system. In the refinement machine, we have refinement on invariants and events. The refinement machines define the conditions on co-owned data sensitivity and users' reputations for either allowing the flow of co-owned data or disallowing the flow.

- $(\forall\, d \cdot (d \in reshared \land class[sensitivity] >$
  $(\forall\, u \cdot (u \in members \land class[reputation]))) \implies (u \mapsto d \notin access)$
  $((\forall\, d \cdot (d \in reshared \land class[has(d)]) >$
  $(\forall\, u \cdot (u \in members \land class[reputation(u)]))) \implies (u \mapsto d \notin access)$

Given expression summarises the purpose of the developed framework's control point. It does not allow flow of any element of co-owned data, which has high class sensitivity, to any user in the system, whose reputation has lower class value than co-owned data sensitivity class value. The class values of the reputation and the class values of the co-owned data sensitivity are given on Table 7.2.

Figure 7.3 illustrates the structure of re-sharing control in the system. As it is aforementioned that the developed framework checks re-sharing of the shared co-owned data *only if* the owner wants to control future flow of the data. When the first group of users (*the first targeted group*) access the shared co-owned data and intends to share it with the new group of people, the control machine starts fine-grained checking on the co-owned data

sensitivity and the users' reputation, who are in the new targeted group, whose members are intended to have permission to access the shared co-owned data. Fine-grained control means that new sharing is individual, not group-based. The data is available to only those users whose reputation' class value is greater than the co-owned data sensitivity's class value.

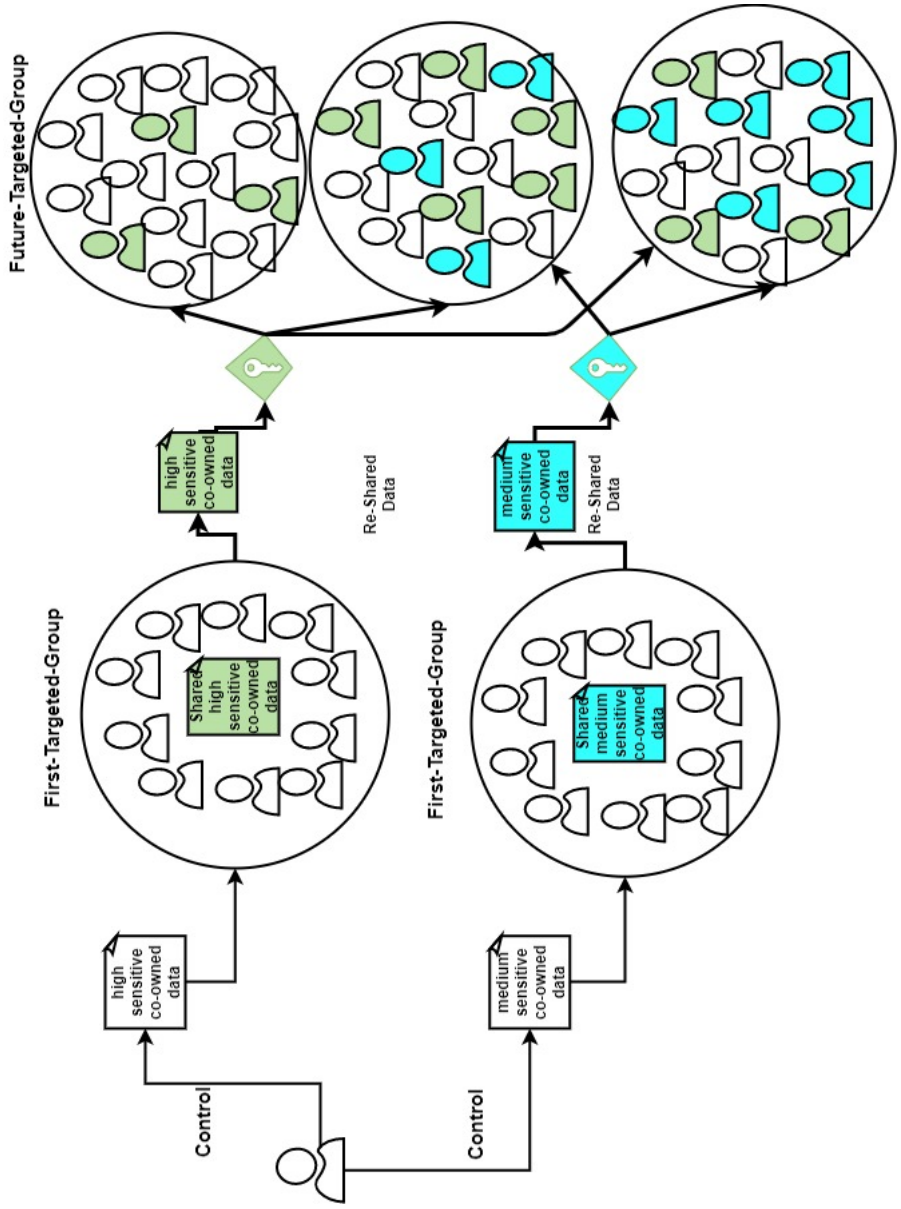

Figure 7.3: Control Machine Re-Sharing Control Structure

Algorithm 5 controls the re-sharing for the future flow of co-owned data with the co-owned data sensitivity value and users' reputation values. If the data is considered high sensitive by co-owners, while it was being shared, then the further users' reputation value has to be high for being permitted to access the co-owned data. This means that any user, whose reputation is lower than the specified value, can not have access to the co-owned data when it is re-shared. Re-shared means here as it is explained before that the co-owned data flows from first targeted group to new groups. The next case is that the data is considered not highly sensitive but medium sensitive. In this case, further users' reputation value has to belong to the medium reputation class. Access is being denied to users whose reputation value is less than medium reputation class value. Low sensitive data is being permitted to any users in the system. This is because the shared co-owned data is not considered as a content which might cause a privacy issue for co-owners, while the co-owned data was being shared by the owner fort he first targeted group.

7.6 Conclusion

Formal modelling is an advantage for expressing good properties of specification and proving the obligations in a system. Therefore, this chapter has presented formal modelling and verification of controlling of shared co-owned data future flow by using Event-B formal modelling language. OSNs' platforms have commonly been used by people, people communicate to each other via data. OSNs' users are let to control the flow of data for the first targeted group, however, they do not have control of flow once the data is on the targeted group's people hands. In this chapter, we have first shown the problem of the current OSNs on controlling shared contents of co-owned data. Our approach aims to assign the reputation values to users and sensitivity values to co-owned data and use

Re-Sharing Control of Co-owned Data for Further Users;
input : d_i
output: $Access = Permit/Deny$

d_i *reshareddata*:
if $d_i \in$ *co-owned* **then**
  if $Sd_{di} > 0.7$ **then**
    for $i = 1$ **to** n **do**
      if $rept_{[ui]} \geq 2.9$ **then**
        Access$[u_i \mapsto d_i] \implies$ PERMIT
      else
        $Access[u_i \mapsto d_i] \implies$ ***DENIED***
      end
    end
  else if $0.4 < Sd_{di} \geq 0.7$ **then**
    for $i = 1$ **to** n **do**
      if $rept_{[ui]} \geq 1.3$ **then**
        Access$[u_i \mapsto d_i] \implies$ PERMIT
      else
        $Access[u_i \mapsto d_i] \implies$ ***DENIED***
      end
    end
else
  $Access[u_i \mapsto d_i] \implies$ ***PERMIT***
end
return: Re-Sharing Control is Done

Algorithm 5: Algorithm: Re-Sharing Control of Co-owned Data for Further Users

those values for controlling co-owned data flow in OSNs. Formal modelling in Event-B allowed us to completely define and verify the control flow and prove the accuracy of the flow control of shared coowned data. In this Chapter, we use OSNs platforms as a case study, however, the specifications and functions are enough general to cover not only OSNs but also any system that has similar features with the proposed work.

This chapter of the thesis contributes to existing knowledge of OSNs' data flows by providing a way of controlling the future flow for shared co-owned data in OSNs. We have shown that how to take an OSN to present the use of Event-B, for not just changing states, but also controlling movement of shared co-owned data. This chapter has also explained in detail a shared co-owned data control flow to make sure that the high sensitive data never flows to people whose reputation values are not high.

Chapter 8

Trusty: System Architecture And Implementation Details of The Developed Framework

This chapter explains the verification of the developed models in Chapter 4, Chapter 5, Chapter 6, and Chapter 7. In Chapter 1, Figure 3.2 represents a complete view of the proposed framework for secure sharing co-owned data process.

This chapter also shows the applicability of the proposed models with a real life web-application. None of the previous works in the area attempted to apply their developed models in a practical implication. The theoretical implication is the most crucial point to solve a problem in a research, however, the practical implication is the way to prove that the theoretical models work in the correct way. The practical implication also ensures the applicability of theoretical models. We therefore implement this thesis theoretical models, which are given from Chapter 4 to Chapter 7, in this Chapter. Implemented online web-

site works with developed fuzzy logic-based decision making, consensus-reached group decision making, and users' trust and reputation values. It also controls the shared content of co-owned data with regards to users' reputation values and co-owned data sensitivity value (Chapter 7' contents). The implemented online social network has been named with the *Trusty*. As it is aforementioned that the *Trusty* comprises of the implementation of the works introduced in the previous chapters.

8.1 The System Requirements

There are main functional and non-functional requirements which need to be covered by the system in order to present the system is the implementation phase of this thesis. We now explain the functional non-functional requirements. Functional requirements describes what a software system should do, while non-functional requirements place constraints on how the system will do soOlsina and Becker (2018). For example, a functional requirement would be a system must send an email whenever a certain condition is met while a non-functional requirement for the system may be emails should be sent with a latency of no greater than 12 hours from such an activity. With regard to the above definition of requirements and example, we now give this thesis implementation system's functional and non-functional requirements.

Functional requirements are as follows;

- The system must calculate data sensitivity value with the probability of chosen data security features
- They system must calculate the relation value and confidentiality value

- The system must use the developed fuzzy logic-based decision system
- The system must provide an output from the fuzzy system
- The system must use group decision making system
- The system must use trust values to weight co-owners' opinions in group decision making process
- The system must use the EIOWA technique for group decision making
- The system must provide an output from group decision making system
- The system must compare the output from fuzzy logic system and group decision system
- The system must provide a feedback to co-owners and the owner
- The system must calculate trust loss and trust gain for each co-owner in a co-owned data sharing process
- The system must provide trust loss and trust gain values in each co-owner to the owner
- The system must calculate the owner's reputation value at the end of the sharing process
- The system must control flow of shared co-owned data if it wants to be controlled
- The system must allow users to share types of contents, such as video, photo, and text.
- The system must allow users to have an account

- The system must allow a user to send friend request to others users on it
- The system must allow users to tag other users in a co-owned data sharing process
- The system must send notification to users if they are tagged on a co-owned data sharing process

Non-functional requirements of the system are as follows;

- Users should be able access to their accounts whenever they want.
- The system should have enough domain for ensuring that the number of users is not restricted as same as other online social networks
- The system should have a document which gives an explanation of the system
- The system should protect users' privacy
- The system should use the developed framework for its quality and reliability
- The system should give notification once a user's name is appeared on a co-owned data sharing process

8.2 Architectural Details of the Implementation

This section gives an explanation of the design steps of the implementation of the developed framework along with the developed mathematical models. The core activities for implementing the developed framework are; requirements, analysis/ planning, design, coding/ programming, testing, and deployment. The first activity taken in the development process is to identify the requirements of the system. This phase produces a

complete and specified requirements of the system. In the analysis phase, the additional requirements are defined and the most crucial part of the software are analysed. The interface of the system and the design of the database tables are covered in the design phase. The programming/ coding is initiated from the design phase but the entire coding, which is required to implement the system, is done in the programming phase. The deployment phase is the last step of the implementation. When all requirements are met in the implemented system, the system is released to its users. All phases are tested before moving to the next steps. Figure 8.1 presents the steps which were taken in the designing process. The first step taken was to document the system requirements and then evaluate the documented requirements. The evaluation is a very important step as it helps to check whether all requirements of the system are covered or not. After being satisfied with the system requirements, we moved to the second step in the figure, which is designing the architecture of the system. At this point, we analysed the appropriate programming language and the database requirements and database design. Defining database requirements need a deep analysis on the system requirements, therefore, it is important to review the system requirements at this point. When designing the architectural structure of the system was completed, designing the user interface of the system was initiated. At this stage, coding was started. In terms of Database Management System (DBMS), My Structured Query Language MySQL was chosen, which is one of the the world's most popular open source databases MySQL (2001). The web application was implemented using PHP. Evaluation of the generated detailed design was checked. It is important to highlight that the evaluation was done *offline*. After completing the coding and interface design, implementation was tested. In order to test the generated design, three test users' accounts were created to test the designed system with test accounts. The testing phase was done when the system was *offline*, which means that the system is not available to the real world users, yet. All testing, evaluation, and revision steps helped us to realise the incomplete parts in

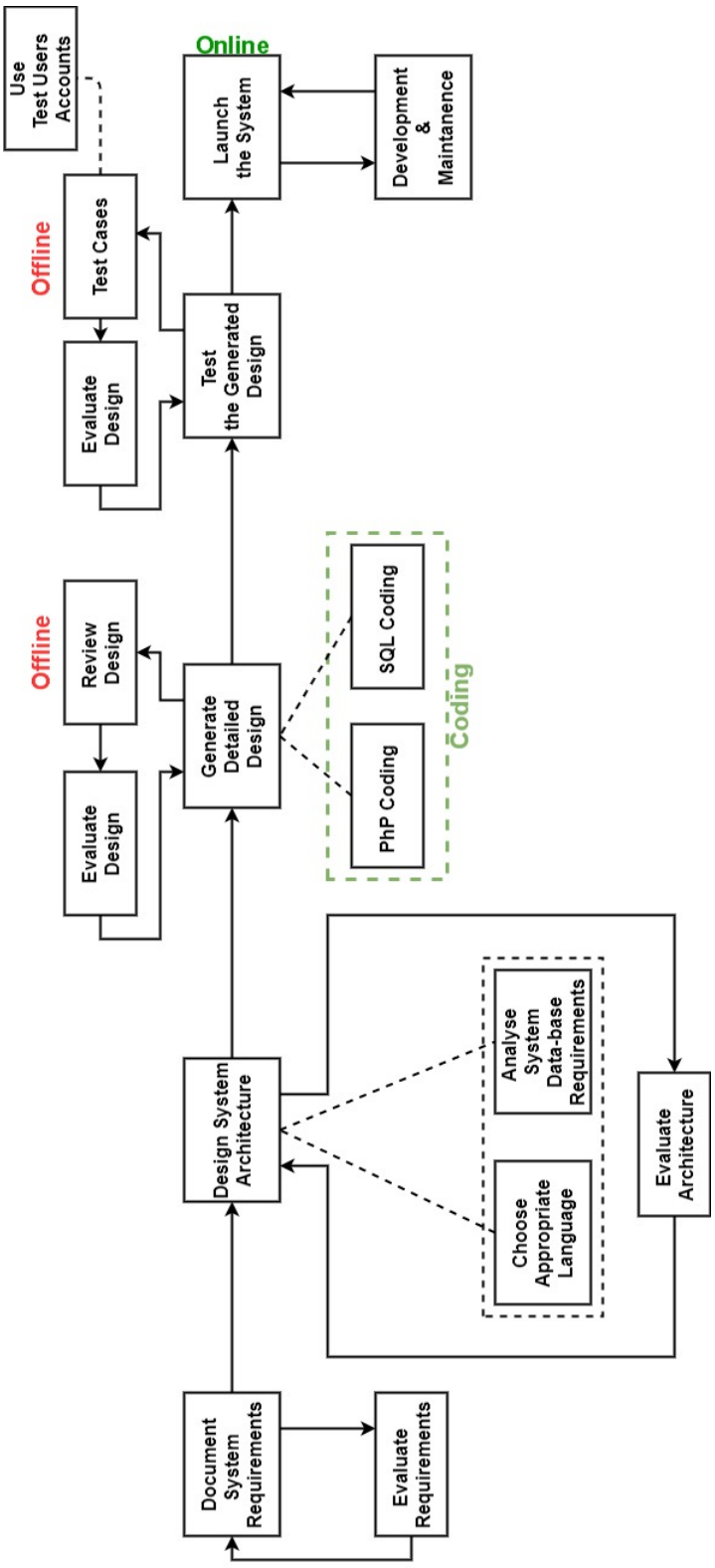

Figure 8.1: The Implemented System Model

the designing stage of the system. The last step in the designing phase is to launch the system. From this point, the system has become accessible to real world users. We have kept developing and maintaining the system after the last step is taken (see in the figure *Launch the System* step).

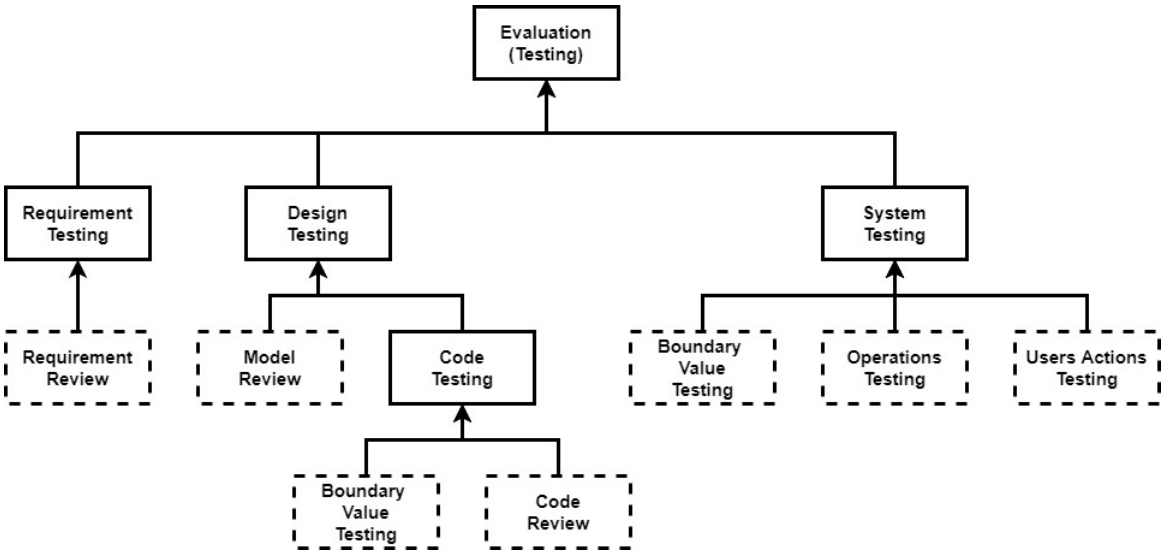

Figure 8.2: Evaluation Assurance Steps

Figure 8.2 presents the details of the evaluation phases given in Figure 8.1. The testing phases given in Figure 8.2 are crucial steps in the implementation and the designing of the proposed work. The requirement testing is the backbone for the implementation and the designing. The reason is that all information used in the designing and implementation comes from the requirements analysis. In the *Design Testing*, there are two main phases; *Model Review* is used to review the developed models in the thesis. *Code Testing* consists of two sub phases namely *Boundary Value Testing* and *Code Review*. Boundary values in the developed mathematical models are tested in this phase and written PHP code is tested gradually. *System Testing* consists of three sub phases which are *Boundary Value Testing*, *Operations Testing*, and *Users Actions Testing*, respectively. The boundary value testing is an analysing technique which is used to test the boundary values in a range. As it is

aforementioned that the developed mathematical models in this thesis have range boundaries, therefore, the boundary value testing is required in the system testing. We used the *Operational Testing* in order to evaluate the operational readiness for the developed system application to release the developed system. *Users Actions Testing* is used to evaluate the implemented work of this thesis. At this stage of testing, the main requirement for the implemented work is to interact with the real life users and meet all the requirements of users actions in the implemented system.

8.3 Trusty Online Social Network

This section gives a detailed explanation of developed models implementation in this thesis. It also gives the sequence diagrams of the implementation phase.

What is the *Trusty*?

The *Trusty* is a web-based online social network system, which allows users to get accounts, interact with other users, share information, express opinions for making decisions on a data sharing process, make consensus-based group decision, and control a shared co-owned data. Table 8.1 presents various information about the *Trusty* including its web address, its source code location, the number of users on it, and the number of friends on it. User Manuel document is placed in Section A.2 in Appendices. It also presents all related actions on the *Trusty* that can be done by its users.

Table 8.1: *Trusty*'s Information

Trusty Address	`http://www.trusty.gen.tr/`
PHP Source Code	`https://github.com/gulsumakkuzu`
The number of nodes	4300
The number of edges	1100

Unified Modelling Language (UML) is the well-known modelling language in the field of object-oriented software engineering Ohst et al. (2003). UML diagrams are designed to help developers to view a purposed system from different perspectives. There are various types of UML diagrams such as use case diagrams, class diagrams, interaction diagrams, and state diagrams. In order to implement the *Trusty* online social network system, we created use case diagrams, class diagrams, and sequence diagrams, which is a type of interaction diagrams.

Use Case Diagrams of the *Trusty* System

A use case diagram is used to present interactions between a user and the system. In a use case diagram, there are two main components which are use cases and actors. Actors are users who use the developed systems. In the *Trusty*, there are two types of actors; one is the owner of co-owned data and the other one is the co-owner. Use cases represent actions the owner and the co-owner perform in order to complete a co-owned data sharing process in the *Trusty* system. Figure 8.3 presents the use case diagram of this thesis. The use case diagram is a set of states that displays the interaction between users and the system. There are two roles for users in this thesis, one is the owner and the other one is the co-owner. It shows the relationship between use cases and actors.

Class Diagrams of the *Trusty* System

Class diagrams are used to describe the types of objects in the *Trusty* system and also the relationships between the class diagrams. The class diagrams of the *Trusty* system are used to describe the conceptual specification of the system when it was being designed. Figure 8.4 shows the class diagram models of the *Trusty* system. Class Diagram models are used to illustrate different types of objects and their relationships using design elements such as packages, classes, and objectives. In the UML diagram of the system, there are nine classes in total. Two classes are not connected to the other classes in the system

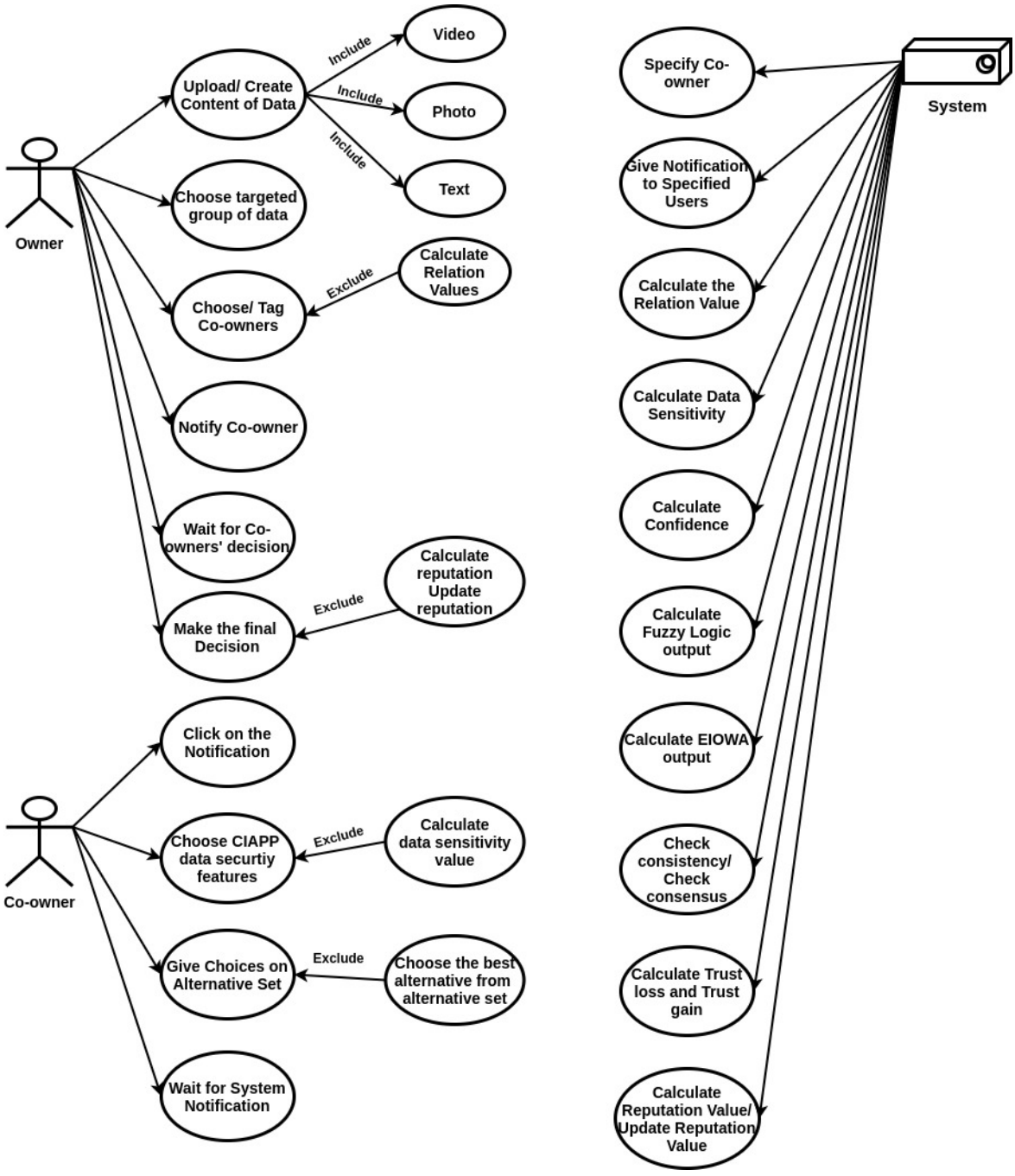

Figure 8.3: Use Case Diagram of the System

structure while other seven classes have relationships among them.

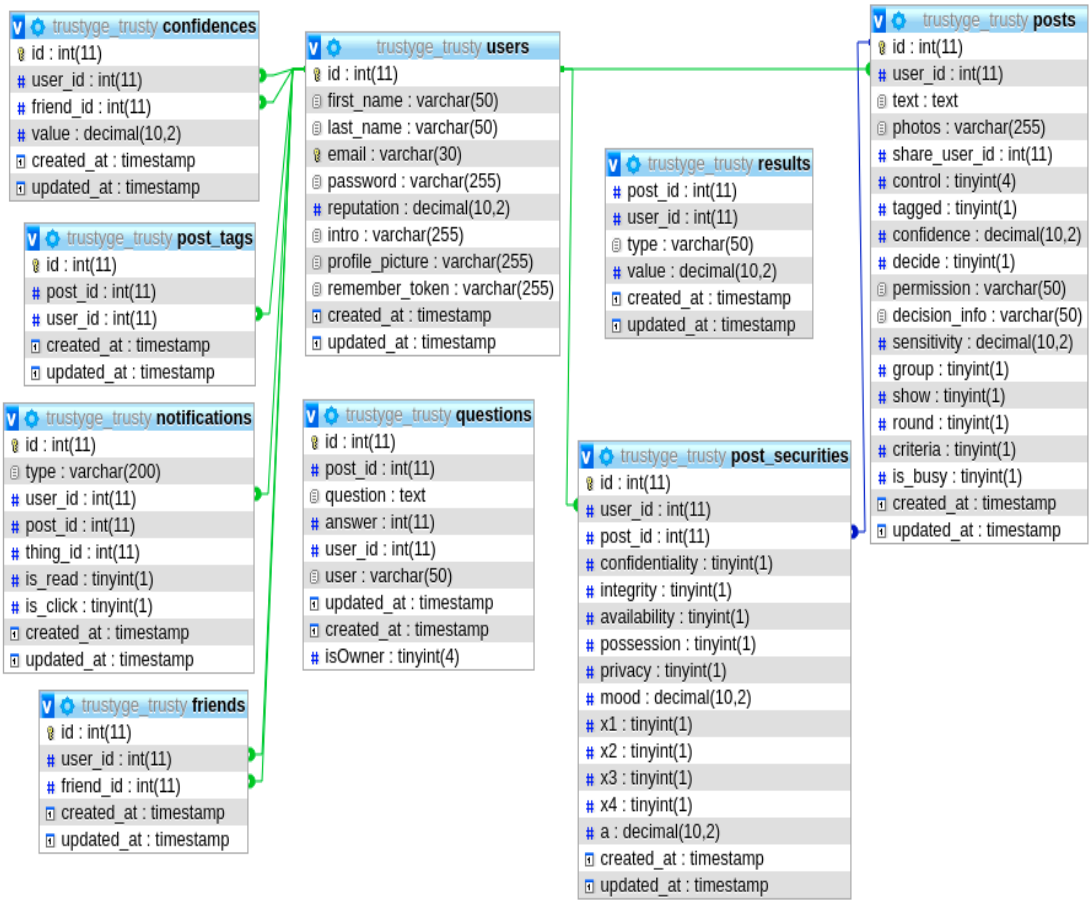

Figure 8.4: Class Diagram of the Trusty System

Sequence Diagrams of the *Trusty* System

In a system, sequence diagrams are used to demonstrate the behaviour of objects in a use case with the description of objects and the messages they pass. The way of reading diagrams in the system is left to right. The *Trusty* system's objects are the owner, the co-owners, and the system itself.

Figure 8.5 presents the sequence diagram of the implementation. There are three actors in the diagram, namely *Owner*, *Trusty*, and *Co-owners*. The system plays the main role of any action in the sequence, for example, the system is responsible to carry all the

actions are made by any users on it. The system notifies the owner and co-owners in a co-owned data sharing process. The owner starts a co-owned data sharing process by either uploading contents of data, making contents of data, or creating a text in the system. The owner then specifies the targeted group for the data and chooses co-owners (*i.e. tags co-owners*). The system takes the next step to notify co-owners and gives them the options to allow them make their choices on *CIAPP* data security features and the fuzzy alternative set. Detailed explanation of sequences between co-owners and the system are given in Figure 8.6. The system checks the consistency between two outputs of fuzzy systems when all co-owners response the owner's request in co-owned data sharing process. The system is responsible for all calculations which are given in Chapter 4, Chapter 5, and Chapter 6. The system is responsible to transmit all notifications between the owner and co-owners. A co-owned data sharing process is ended by the owner with a final step, which can be either respecting co-owners or ignoring the co-owners group decision in a co-owned data sharing process.

Figure 8.6 shows the sequence diagram which represents steps between the system and co-owners. Co-owners are responsible to give their choices on the *CIAPP* security features and the fuzzy alternative set. If the consensus is reached and consistency between two fuzzy sets is achieved, then co-owners do not have any more responsibilities. However, if the consistency is not achieved, then the co-owners have to choose the CIAPP and make their choices on the alternative set. Figure 8.7 and Figure 8.8 are the representations of the *Trusty* class diagrams with the time sequence. The time sequence is used to demonstrate the time difference among events in the *Trusty* system. In the system, the actions of actors come sometimes one after another. There are also some actions occur parallel, especially co-owners actions occur in parallel (see 8.8).

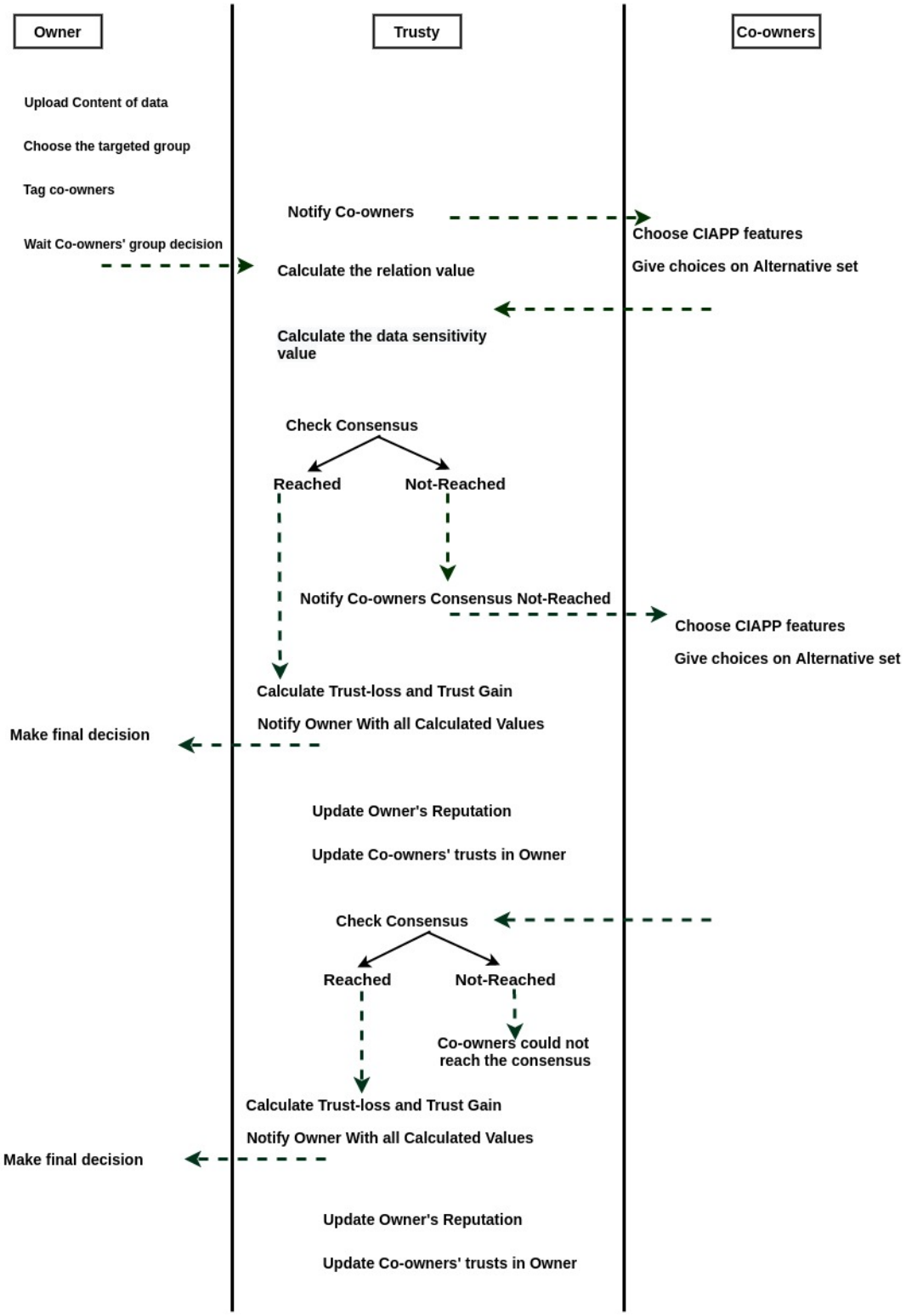

Figure 8.5: Sequence Diagram of the the Trusty system

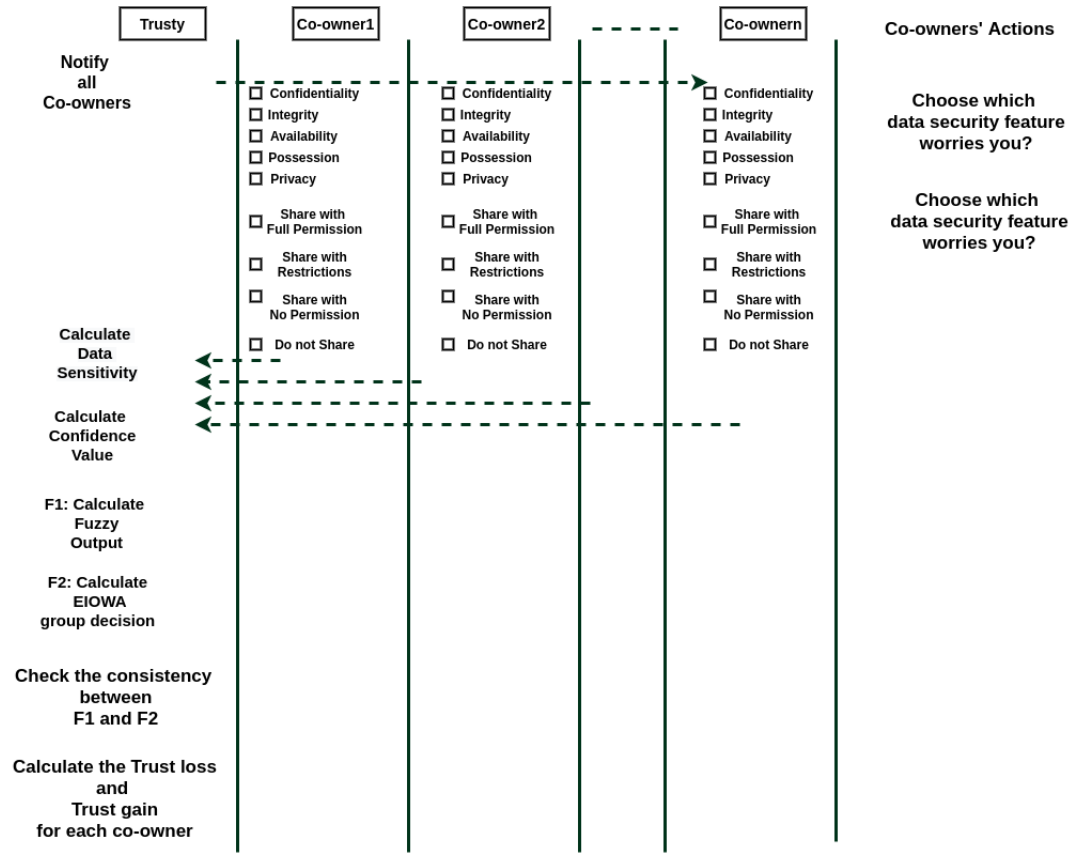

Figure 8.6: Sequence Diagram for Action Between Co-owners and the Trusty System

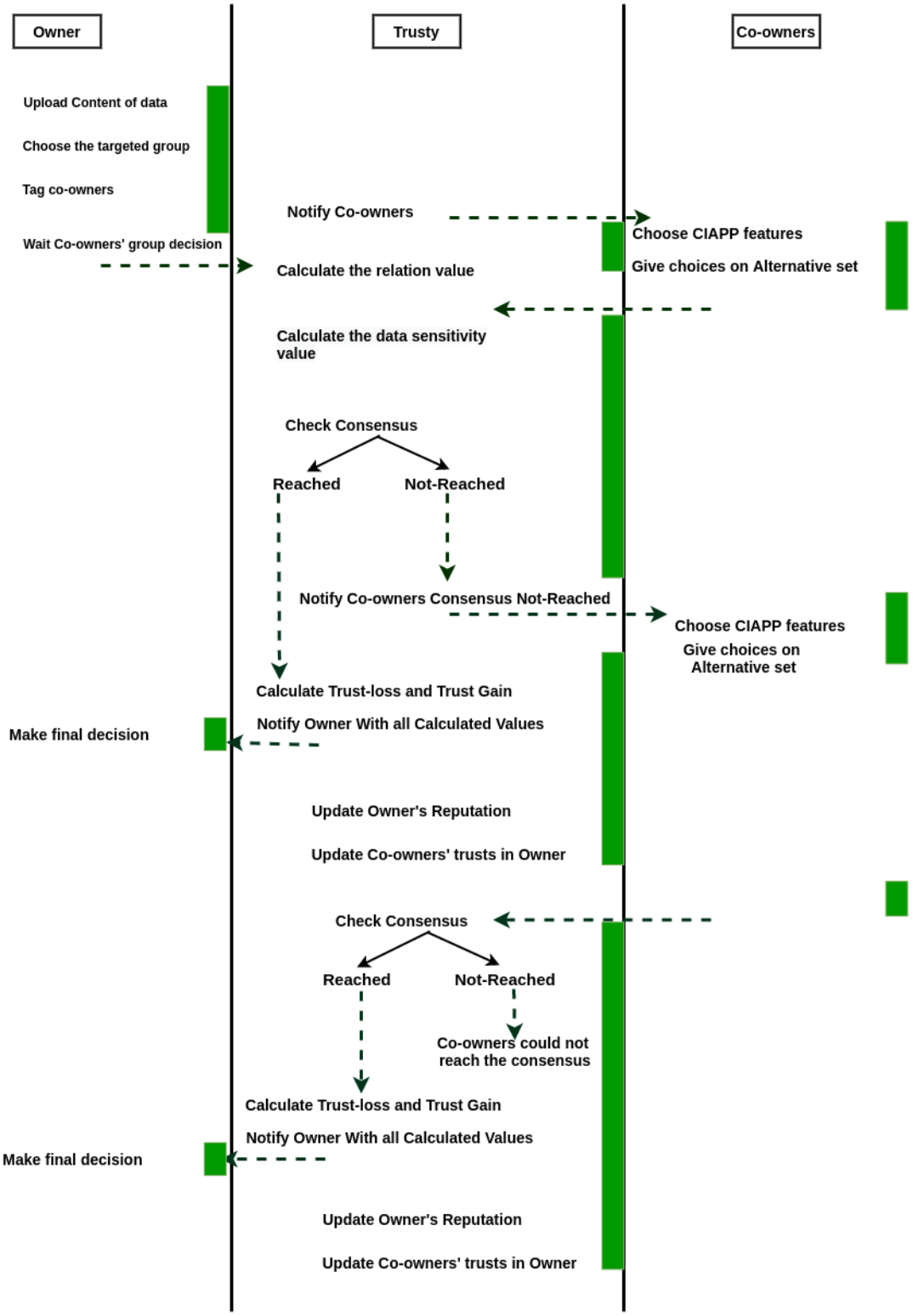

Figure 8.7: Sequence Diagram of the the Trusty system with Time Sequence

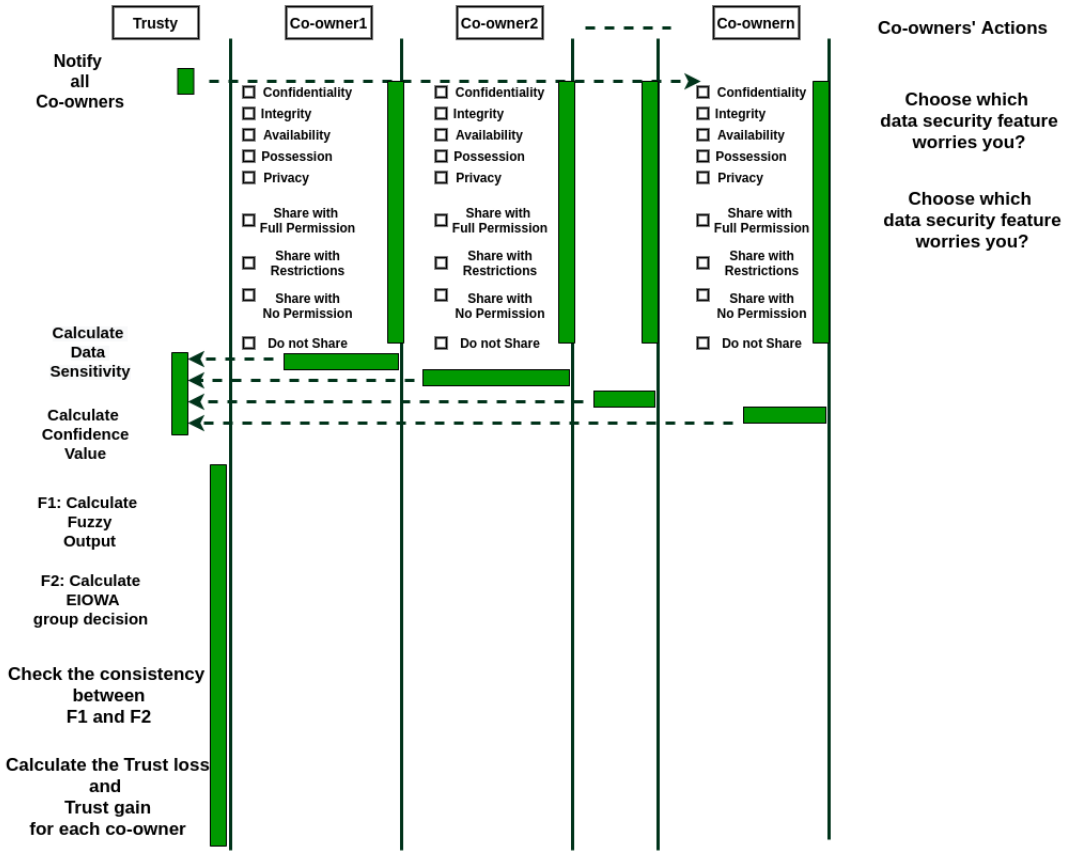

Figure 8.8: Sequence Diagram for Action Between Co-owners and the Trusty System with Time Sequence

8.3.1 Evaluation of the implementation; Trusty Online Social Network

In order to evaluate whether the *Trusty* system satisfies the specified requirements or not, testing is required. The main requirement of the *Trusty* is that the social network must work with the developed models which are developed in this thesis. The system must cover the specified functional and non-functional requirements for its evaluation (see Section 8.1. The functional requirements are mainly used to evaluate the implemented work, each functional requirement is checked in the evaluation process. For example, the system must use the fuzzy logic-based decision with the developed equations; this requirement is used to evaluate the implemented system. This means that each value in the developed equations are checked to see whether equations are implied correctly or not. The same criteria is applied to each functional requirement and the functional requirement is evaluated with regard to its specifications.

The system testing has been started from the beginning of the implementation in order to determine the incompetent points in the implementation phases. On each step of the implementation, the testing has been done with different approaches. For instance, in the designing phase, the testing has been used to improve the design. The testing of the implemented work has been finished when the coding has covered all the functional specifications of the developed framework. The way that the *Trusty* online social network has ensured that the developed social network has met all the functionality, and verified that the *Trusty* online social network has been built correctly. After completing the verification, the validation of the *Trusty* online social network has occurred for checking of the overall the *Trusty*. The evaluation of the *Trusty* online social network has been considered from a subjective perspective.

The implementation part of this thesis has two goals; one is to present the applicability and usability of the developed models in real world applications and the other one is to deduce the needs of using group decision making and having users' trust and reputation values in co-owned data sharing processes. The applicability of the developed models has shown via the *Trusty* online social network. In a typical online social network, there are behaviours which could be done by any online social networks' users. These typical user behaviours are specified by Amato et al. (2018); the specified behaviours are *log-in, profile settings, search friends, messages, photos, shares, like, comment, and log-out* namely. *Trusty* online social network has all the specified typical user behaviours that any online social network needs to provide to its users. However, the *Trusty* has main difference on co-owned data sharing processes. Co-owned data sharing requires group decision making and fuzzy logic-based decision making system in order to make a decision in the sharing process.

8.4 Conclusion

This chapter covers detailed explanation of the design, implementation, and analysis of the developed framework with its mathematical equations. We give the evaluation of the implemented work with a subjective evaluation.

The implementation was done through an online social network platform. The strong points of the implemented work are as follows. The first strong point is that in *Trusty* network, co-owned data sensitivity is decided not only by the owner but also co-owners have chance to give their opinions on the *CIAPP* data security features. This is because data sensitivity is an individual aspect, therefore, each user, whose information is involved into a co-owned data, has their own concerns in co-owned data sharing process. The

second strong point is that *Trusty* uses the data security features to calculate co-owned data sensitivity values. The used data security features are as follows; Confidentiality and assurance that only authorised people can access data. Integrity ensures that the data is an accurate and unchanged representation of the original secure information. Availability ensures that the information concerned is readily accessible to the authorised viewer at all times. Possession ensures that ownership and control of data is in the hand of or under the control of possessor. Privacy ensures that the collection and dissemination of data is legal. The third strong point on *Trusty* is that a fuzzy logic-based decision making system is used to disambiguate in decision making when a content of data is very sensitive and confidence in data targeted group is high. Another strong point is that in *Trusty* network, a fuzzy group decision making is used to choose best option among given alternatives in order to share a co-owned data content. In the proposed group decision making system, users trust values for each other are used to weight their opinions. The last powerful and strong point is that in *Trusty* network, users trust and reputation values are used as a reward or punishment when the owner shares a co-owned data content by respecting the co-owners decision or ignoring their decisions. The implementation of the proposed work has shown that it is an important need to use fuzzy decision systems and users trust and reputation values in co-owned data sharing processes in OSNs.

Chapter 9

Conclusion and Future Work

The use of online social networks has remarkably increased in the last decade and this increment has increased information sharing. The information-sharing sometimes is related to more than one user without letting involved users know about this. Such cases have brought challenges in making the decision on sharing contents of data which leads to ongoing research on privacy. This thesis was motivated by the observation that existing privacy issues which are originated from co-owned data sharing. The observation showed that the reason for having privacy issues in co-owned data sharing processes is that the current online social networks do not have a structure which uses group decision making in a co-owned data sharing process. The current online social network platforms also do not have any method to punish a user if the user causes privacy leakage with sharing co-owned data. These needs led us to develop a framework in which the fuzzy group decision-making process and punishment/rewarding system are used in co-owned data sharing processes. The developed framework and mathematical models, which have been developed in order to achieve the aim of the proposed work, are illustrated in the contributions of this thesis.

9.1 Evaluation of The Proposed Work

This section covers the evaluation of this thesis work. There is no evaluation based on performance or any other quantitative metric because we are not aware of a suitable metric to evaluate the framework with a quantitative metric. Therefore, the developed framework and the developed models have been evaluated technically and critically. The critical evaluation was done with a comparison between the developed models and a similar work in the literature. In this section, the developed models have also been evaluated technically. The technical evaluation has been done by looking back to the research questions and the achievements of this thesis.

This section is an attempt to evaluate the developed framework, we have used some measurable metric to validate the proposed work. Two constructive assessment are used to justify the outcome of this thesis. The first evaluation technique is the technical validation technique, which is used to test the functionality of the developed models Leijnse and Hassanizadeh (1995) against the research questions given in Chapter 1. Implementation technique is used for evaluating the developed models and the usability of the framework. Implementation is one of the main part for verifying and validating developed models Sargent (2010). The first step is to check the models' operational behaviours with graphical displays. In this thesis, each developed models' behaviours are shown in the chapters in which models are given. We also did parameter variability analysis by changing variables of parameters in the models in order to determine effects of different variables on the models' behaviours and outputs. Coding/ programming is the way of verification of the validated models, we use the structured walk-through technique for the implementation. The structured walk-through technique is the common technique for model verification Sargent (2000), it ensures that the developed models are validated and used in the imple-

mentation with a real world application. The real world application's evaluation has been carried out with users interactions (*i.e. users evaluations*) on the proposed work.

The second approach is critical comparison between the developed framework and related works. Critical evaluation is used to evaluate the proposed work with the related works on the cases of similarities and differences Vartiainen (2002). This thesis comparative evaluation factors are similarities and differences of concepts, definitions, and mathematical modelling.

9.1.1 Critical Evaluation

In this section, we compare this thesis work with similar research works, which have been proposed by Xu et al. (2018), Ulusoy (2018) and Takalkar and Mahalle (2018), in the literature. The chosen research works also aim to protect users' privacy in data sharing processes. Evaluation components are architecture, interoperability, operational capabilities, and the obligation capabilities. Details of each component are as follows;

Architecture

Based on the architectural structure, there is just one work that can be compared to our work, *Xu et al.* work is used to make comparison. Xu et al. (2018)' study and this thesis have similar architectural structure with respect to taken steps in a content of data sharing process. For example, in both studies, the initiator of a sharing process is a person, who is called data owner. Both research studies aim to complete a data sharing process with no privacy leakage. In both studies, the data sensitivity value is used for common data, but while the data sensitivity value is used with one hand in the compared study, the data sensitivity value is associated with the users involved in the data sharing process in the proposed work. Both studies also use the reputation and trust values with their own

developed models.

There are various differences between two works architectural aspects, for instance, this thesis work has used a *fuzzy-logic decision* expressions while the compared work used *Boolean logic* expressions. This thesis uses a consensus-reached group decision while in the compared work there is no consideration of consensus-reached group decision making in co-owned data sharing process. The proposed work also uses a fine-grained shared co-owned data flow in order to guarantee that the shared sensitive data never flows to low reputed users, whereas, the compared work does not have any concerns on the control flow of co-owned data.

Usability and Interpretability

It is important to implement formalised models with a real-world applications, which represents the applicability and usability of developed models and the proposed work. The compared work has not implemented its developed models while this thesis has implemented its developed models in a real-world web application.

The interpretability of research models is an important factor for obtaining more accurate and similar systems to real life models. This need in research area can be achieved with the usage of fuzzy models, therefore, this thesis framework is more transparent and interpretable. Because, fuzzy decision making systems are used in the developed framework. Fuzzy rules and variables can be interpreted and adjusted based on the specifications of any system. Also, fuzzy systems have ability for interpreting the relationship between input and output variables.

The adaptability of the developed framework and simplicity of the implemented online social network (*i.e. Trusty*) are important factors for usability evaluation. The developed can either be used as a whole structure or partially in co-owned data sharing process. The

fuzzy system, which is introduced in Chapter 4, has already been used in a data sharing process in the Internet of Things area by Scheidt et al. (2020). As it is mentioned above the simplicity of the *Trusty* online social network is the criteria for usability evaluation. The implemented online social network has not only satisfactory activities but also has a widely interface.

Operational Capabilities

In this work and the compared research works, the privacy issue is taken from the same perspective. This means that compared research works and our work have focused on the privacy issues which are derived from co-owned data sharing in OSNs. Compraed works except *Xu et al's* work did not use reputation system to protect users' privacy in OSNs. *Xu et al.*'s work and our study have aimed to use the users reputation values, however, the models are completely different in both studies. In the compared work, the trust models are doubt-able, especially the trust gain model. The model is a function which has privacy loss value and previous trust values to calculate the next trust gain value in a user's account, however, it does not increase the trust value if someone does not have privacy loss in the model. Therefore, this thesis work has approved all the developed models behaviours in order to demonstrate the correctness of the models.

Obligation Requirements

Considering that privacy issues, which are caused by co-owned data sharing in OSNs, it is an important issue because it makes users to either be unfriend with users, who cause a privacy issues, or quit from OSNs platforms. It requires a technical solution which aims to make a balance between co-owned data sharing and privacy protection. This shaped the development of a mechanism that uses users opinions in data sharing process and uses a punishment and rewarding system. The developed framework has used the necessary aspect for more secure co-owned data sharing processes in OSNs.

9.1.2 Technical Evaluation

In Chapter 1, four research questions were developed in order to achieve this thesis main aim on having a framework which can make a balance between co-owned data sharing and privacy preserving. Based on the main research question, the developed framework needs to be general enough to fit into any environment where the privacy protection and data sharing are required. Therefore, we look back to the main question and the developed framework to verify and assess the technical usefulness of the developed framework and the functionality of mathematical models.

1. Fuzzy-Logic Based Decision: OSNs reflect peoples' real lives with various contents such as shared photo, video, location, events, and friends Akhtar et al. (2018). However, the expressions that are used in decision making in OSNs are not similar to the real life decision expressions. Fuzzy-logic was proposed by Zadeh (2008) in order to make decision expressions as similar as real life decision expressions, therefore, we use a fuzzy-logic based decision making system in the developed framework.

2. Consensus-reached Group Decision Making: Reaching consensus is important in group decision making processes since it indicates that the group was able to make an aggregated decision with an appropriate choice. In this thesis, a consensus-reached group decision making technique is used to make sure that group's decision does not cause any privacy leakage in co-owned data sharing process. Therefore, we can say that it is one of the main components to achieve the main goal of this thesis.

3. Usage of Trust and Reputation: The main aim of this research is to protect users privacy when users are involved into co-owned data processes. The proposed work uses a penalising and rewarding system in which users' reputation and trust values

are used. The usage of users trust and reputation values are changed only if data is co-owned. Developed models that are used to calculate trust and reputation values are given in Chapter 7. Each model's behaviours are also given in the chapter. It is important to mention that all developed models of the thesis are used in the real-world application.

4. Controlling Flow of Shared Co-owned Data: Controlling shared contents is an important attempt to know the flow of shared data. It is mainly knowing who will be accessing the contents after the content is shared. In this thesis, we provided formal way of controlling shared co-owned data. In the provided formal modelling, we aimed to protect sensitive shared co-owned data being flown to the low reputed users in OSNs.

9.1.3 Addressing The Research Questions

In Chapter 1, four major research questions were proposed:

* **[Main Question:]**

  Is there any way to make balance between c-owned data sharing and users' privacy preserving on co-owned data sharing processes? item[$*$] **[Q 1.]**

  How can we develop a fuzzy logic-based decision making model to make OSNs' co-owned data sharing/ not sharing decisions similar to the real life decision expressions?

* **[Q 2.]**

  How can we use group decision making process in co-owned data sharing processes?

* **[Q 3.]**

  How can we develop reputation model in OSNs?

Main Question

This question is answered in this thesis from Chapter 4 to Chapter 8, where all requirements, gaps, and challenges for making a balance between co-owned data sharing and preserving users' privacy in OSNs with a framework. The identified requirements, specifications, and challenges are specified in co-owned data sharing processes. Developed framework is implemented in an OSN platforms, named *Trusty*, to represent the usability of the framework in a real world web-application.

Question 2 (Q 2)

This question is fundamentally answered in Chapter 6 with a combination of Chapter 5, where a consensus reached group decision making model is introduced that addresses the usage of trust values for weighting groups' members opinions in a group decision making process. One of the most common and/or grounded technique for group decision making technique is used to develop the proposed consensus-reached group decision making in this thesis.

Question 3 (Q 3)

This question is answered in Chapter 6, where trust and privacy values are used to develop reputation models. In order to update trust loss and trust gain values in the developed reputation equations. The developed reputation models are general enough to use in any systems which includes feedback values.

9.2 Contributions

This thesis provides four contributions that form the secure co-owned data sharing framework. These contributions are as follows;

1. fuzzy logic-based decision making and consensus-reached group decision making
    - data sensitivity calculation mathematical model development
    - confidence in targeted group calculation mathematical model development
    - extension on decision expressions with fuzzy systems
    - a novel alternative set for co-owned data sharing processes
2. usage of users' trust and reputation values in co-owned data sharing processes
    - trust loss and trust gain mathematical models development
    - reputation mathematical model development
    - reputation mathematical model for different cases in co-owned data sharing processes
3. Flow control of shared co-owned data
    - A robust flow control approach in co-owned data sharing processes in OSNs

The first contribution is presented in Chapter 4 and Chapter 5, these two chapters focus on using fuzzy logic-based decision making and consensus reached group decision making in co-owned data sharing process. The fuzzy logic-based decision making system requires specifying the input and output variables. In a co-owned data sharing process, the data sensitivity and the confidence in targeted group of data are important variable for making

decision, therefore, it is important to know the data sensitivity value and the confidence value in the targeted group of data. The first step is to develop mathematical equations which are used to calculate the data sensitivity value and the confidence in the targeted group value. We develop the data sensitivity model based on five data security features. The confidence value in targeted group based on: (1) relationship which exist between related users and each users in the targeted group; (2) the data sensitivity value. The developed models are then placed in the fuzzy system as inputs variables. The next step is to compose inputs, outputs, and rules for fuzzy logic-based system. The last step is to place the developed mathematical models into the proposed framework. Chapter 4 consists the contributions, thus far, to have mentioned. Chapter 5 provides a consensus-reached group decision making process for co-owned data sharing processes. The proposed consensus-reached decision making process uses users' trust values to weight decision makers' (*i.e. co-owners*) opinions in a co-owned data sharing process. A novel alternative set for sharing co-owned data is proposed in the consensus-reached group decision making.

The second contribution, presented in Chapter 6, builds upon fuzzy logic-based decision system and consensus-reached group decision making system. It can be considered as a utility system in co-owned data sharing processes. The contribution consists of the reputation and trust mathematical models which are used to award/punish the data owner when co-owned data sharing process is completed. The trust loss and trust gain values are used to calculate the data owner's reputation value in a co-owned data sharing process. The reputation values are required to be explicit values on users' accounts so that the reputation values can help users to have ideas about users' behaviours in co-owned data sharing process. A user's reputation value is changed only if the user takes the owner role in a co-owned data sharing process.

The third contribution, presented in Chapter 7, is in the last part of the developed frame-

work. In the chapter, we introduced a fine-grained model to control flow of shared co-owned data. The developed model guarantees that high sensitive data never flow to low-reputed users. Therefore, the flow of co-owned data is controlled with two specified features namely co-owned data sensitivity and users reputation values.

To summarise, the contribution of this thesis is theoretical and practical. The theoretical contributions are fuzzy systems, reputation system, and formal model with the developed equations. The practical contribution is the implemented part of the thesis. *The Trusty* social network is a unique social network because of the framework which was used in its implementation steps.

9.2.1 Highlights of the Contributions

Sharing contents of data is one of the main purposes for using OSNs' platforms. People share the contents of data which does not only include the user's information, who uploads the content to the OSNs, but might also include other users' information on. Some of users do not like being included on the contents which is shared by other users in OSNs. These users either quit from OSNs' platforms or become unfriend with the users who shared their information. Users are informed about the shared data when the sharing process is ended. They are not allowed to make a decision while the content is intended to be shared. Some of the OSNs' platforms allow users to remove their information from the shared content however the content is still available on the other users' spaces.

In order to address the above significant and challenging problems on data sharing in the OSNs' platforms specifically co-owned data sharing, this thesis makes four major contributions.

1. The first contribution of this thesis is applying fuzzy logic-based decision making in OSNs' platforms.

   (a) A novel fuzzy-logic decision making is proposed. This new approach contains two crucial pieces of information as input values for fuzzification, including the data sensitivity value and the confidence value.

   (b) We propose a new concept which uses the co-owners' choices on the CIAPP features of the content to calculate the data sensitivity value. The new approach uses the connection among the nodes to calculate the confidence value. The membership values of inputs and output value are decided with the data-driven approach with the K-Nearest Neighbour clustering technique.

2. The second contribution of this thesis is consensus-reached group decision in OSNs' platforms.

   (a) In OSNs' platforms, decisions on the data sharing processes are made by only one user regardless of whether the data are owned by only one user or more users. These type of data sharing cause different problems in OSNs platforms, such as accounts quitting, becoming unfriends, and privacy violations. Multi-handed decision (i.e. group decision) is needed in OSNs' platforms on the data sharing where the data includes more than one users' information.

   (b) To address single-handed decision making in co-owned data in OSNs platforms, we propose a consensus-reached group decision making process on the co-owned data sharing process. Extended induced average weighted techniques is used to make consensus-reached group decision.

3. The third contribution of this thesis is modelling for usage of users' reputation values in OSNs.

(a) We propose a reputation concept that is developed with the beta reputation system.

(b) In the proposed reputation system, we use trust loss and trust gain values as feedback values from the co-owners. The data sensitivity value is used as a weight for the new reputation system.

4. The fourth contribution of this thesis is formal modelling of flow control on shared co-owned data in OSNs.

(a) To address the challenge of controlling the shared data in OSNs, we propose a formal specification and modelling for controlling the flow of shared data. The proposed model shows that it is possible to control the shared co-owned data with the users' reputation values and the co-owned data sensitivity value.

9.2.2 Strengths of the Thesis

The strengths of this thesis are as follows;

- A co-owned data sharing framework; The strength is to have more secure co-owned data sharing processes.
- Robust mathematical models which can be used in any co-owned data sharing process.
  - Co-owned data sensitivity mathematical model
  - Confidence model which measures confidence in data targeted group
  - Trust calculation mathematical models
  - Reputation calculation mathematical model

- A consensus-reached group decision making for co-owned data sharing processes in OSNs

- Usage of users' trust values in order to weight decision makers opinions in co-owned data sharing decision making processes

- Robustness of the control flow of shared co-owned data based on formal proof of properties.

- Implementation of the developed framework and mathematical models in a real world web application. The implemented online social network proves the usability study of the developed framework.

- Analysis on the implemented work with its users evaluations

9.3 Future Work

This thesis has four main contributions that form part of the secure co-owned data sharing framework. The main aim of these contributions was to develop a framework that uses group decision making and users' trust and reputation values in order to make co-owned data sharing more secure. Also, the developed framework aimed to make a balance between co-owned data sharing and privacy protection. This thesis has achieved its purposes with the development of the proposed framework. We now give future directions that can be used to improve the research presented in this thesis.

9.3.1 Extending the Group Decision Making

In this thesis, we have first presented a fuzzy logic-based decision system for making OSNs decision expression much closer to the real life decision expressions. In order to do that, we have presented that the data sensitivity values and the confidence value in targeted group are the effective values to make the decision. Then, we have presented that with the developed fuzzy-logic decision system, we can also use consensus-reached group decision making in order to make the taken decision more convenient. We are convinced that applying fuzzy logic-based decision system and consensus-reached group decision making are necessary requirements to have more secure co-owned data sharing process and satisfy co-owners that their opinions are taken into the consideration when the decision is taken on co-owned data sharing process, which they are involved in. In the proposed consensus-reached group decision making process, we have used users' trust values, which exist between users in order to weight the co-owners' opinions in the decision making process. In this thesis, we used the Type-1 fuzzy systems, however, it would be extended to Type-2 fuzzy inference systems. The group decision making approach would be extended with the usage of unbalanced fuzzy linguistic terms Cabrerizo et al. (2017).

The consensus-reached group decision making was deliberately applied with the EIOWA technique and therefore the main focus was using users trust values in order to weight their opinions in co-owned decision making. It would be extended with other techniques and compare the results of the techniques.

9.3.2 Users Trust and the Reputation Values

In this thesis, we focused on capturing the users' trust values from connection point. In other words, if two users are connected to each other or if there is an edge between two users, then it is assumed that users have trusts in each others. Then, these trust values have been taken from two different perspectives; one is trust gain and the other is trust loss. These trust values change focus on co-owned data sharing process, however, it would be interesting for future improvements to analyse how to capture trust values from more social interactions in OSNs.

Moreover, in this thesis, we have used users reputation values as a way of punishment and reward system. We have seen that people have positive views on having reputation values in OSNs platforms. The reputation changes have only focused on co-owned data sharing processes, however, it would be interesting to analyse more actions which could have effect on users' reputation values in OSNs platforms. In this thesis, a user's reputation value is calculated with the trust loss and trust gain values in a co-owned data sharing process. We are convinced that trust loss and trust gain values can be used as feedback values on a co-owned data sharing process to calculate users reputation values, however, it might be analysed if there are any other features which have effect on the reputation.

In this thesis, the reputation value has been presented with numerical values on users profile, however, this reputation values perspective might be improved where the total number of the co-owned contents posts, which a user have posted on the OSNs and took the role as an owner, can be used as feedback values. For example, the negative feedback could be the number of user's decision which are on the side of the group decision and the positive feedback could be the number of user's decision which are not on the side of group decision.

9.3.3 Modelling the Developed Framework Conceptually

The aim of this thesis is to develop a framework in which there is a balance between co-owned data sharing and users privacy protection. With the evaluation of the work from three different perspectives, which are technical evaluation, critical evaluation, and users evaluation on the implemented work, we are convinced that the developed framework can make a balance in co-owned data sharing and users privacy preservation on co-owned data sharing processes in OSNs platforms. However, it would be good improvement to know how effective is to have the consensus-reached group decision making and users reputation values in OSNs platform to have secure OSNs platforms, where co-owned data sharing processes are more secure. One way to apply this improvement is to develop conceptual modelling and applying confirmatory factor analysis on the conceptual modelling. This thesis framework structure can be used as a motivation to create the theoretical backbone for improvement.

References

Abdullah, L. (2013). Fuzzy multi criteria decision making and its applications: A brief review of category. *Procedia-Social and Behavioral Sciences*, 97:131–136.

Abrial, J., Métayer, C., and Voisin, L. (2005). Event-b language. *Rodin Deliverable*, 3.

Abrial, J.-R. (2010). *Modeling in Event-B: system and software engineering*. Cambridge University Press.

Abrial, J.-R. and Abrial, J.-R. (2005). *The B-book: assigning programs to meanings*. Cambridge University Press.

Acquisti, A. and Gross, R. (2006). Imagined communities: Awareness, information sharing, and privacy on the facebook. In *International workshop on privacy enhancing technologies*, pages 36–58. Springer.

Adoko, A. C., Gokceoglu, C., Wu, L., and Zuo, Q. J. (2013). Knowledge-based and data-driven fuzzy modeling for rockburst prediction. *International Journal of Rock Mechanics and Mining Sciences*, 61:86–95.

Aghasian, E., Garg, S., Gao, L., Yu, S., and Montgomery, J. (2017). Scoring users' privacy disclosure across multiple online social networks. *IEEE access*, 5:13118–13130.

Ahmed, J., Villata, S., and Governatori, G. (2019). Information and friend segregation for online social networks: a user study. *Ai & Society*, 34(4):753–766.

Akhtar, R., Winsborough, D., Ort, U., Johnson, A., and Chamorro-Premuzic, T. (2018). Detecting the dark side of personality using social media status updates. *Personality and Individual Differences*, 132:90–97.

Akkuzu, G., Aziz, B., and Adda, M. (2019a). Advantages of having users' trust and reputation values on data sharing process in online social networks. In *2019 Sixth International Conference on Social Networks Analysis, Management and Security (SNAMS)*, pages 189–195. IEEE.

Akkuzu, G., Aziz, B., and Adda, M. (2019b). Application of extended iowa operator for making group decision on co-owned contents in osns. In *10th IEEE International Conference on Intelligent Systems*. Institute of Electrical Engineers.

Akkuzu, G., Aziz, B., and Adda, M. (2019c). Fuzzy logic decision based collaborative privacy management framework for online social networks. In *3rd International Workshop on FORmal Methods for Security Engineering: ForSE*.

Akkuzu, G., Aziz, B., and Adda, M. (2019d). A fuzzy modeling approach for group decision making in social networks. In *International Conference on Business Information Systems*, pages 74–85. Springer.

Akkuzu, G., Aziz, B., and Adda, M. (2020). Towards secure data sharing processes in online social networks. In *15th I5th International Conference on Software Technologies*. INSTICC Press.

Akkuzu, G., Azizl, B., et al. (2018). Feature analysis on the containment time for cyber

security incidents. In *2018 International Conference on Wavelet Analysis and Pattern Recognition (ICWAPR)*, pages 262–269. IEEE.

Al-Oufi, S., Kim, H.-N., and El Saddik, A. (2012). A group trust metric for identifying people of trust in online social networks. *Expert Systems with Applications*, 39(18):13173–13181.

Ali, B., Villegas, W., and Maheswaran, M. (2007). A trust based approach for protecting user data in social networks. In *Proceedings of the 2007 conference of the center for advanced studies on Collaborative research*, pages 288–293. IBM Corp.

Ali, S., Islam, N., Rauf, A., Din, I., Guizani, M., and Rodrigues, J. (2018). Privacy and security issues in online social networks. *Future Internet*, 10(12):114.

Ali, S., Rauf, A., Islam, N., and Farman, H. (2017). A framework for secure and privacy protected collaborative contents sharing using public osn. *Cluster Computing*.

Alkiviadou, N. (2019). Hate speech on social media networks: towards a regulatory framework? *Information & Communications Technology Law*, 28(1):19–35.

Alonso, S., Pérez, I. J., Cabrerizo, F. J., and Herrera-Viedma, E. (2013). A linguistic consensus model for web 2.0 communities. *Applied Soft Computing*, 13(1):149–157.

Alqatawna, J., Madain, A., Ala'M, A.-Z., and Al-Sayyed, R. (2017). Online social networks security: Threats, attacks, and future directions. In *Social Media Shaping e-Publishing and Academia*, pages 121–132. Springer.

Alsmadi, I., Xu, D., and Cho, J.-H. (2016). Interaction-based reputation model in online social networks. In *ICISSP*, pages 265–272.

Amato, F., Castiglione, A., De Santo, A., Moscato, V., Picariello, A., Persia, F., and Sperlí, G. (2018). Recognizing human behaviours in online social networks. *Computers & Security*, 74:355–370.

Arenas, A. E., Aziz, B., and Silaghi, G. C. (2010). Reputation management in collaborative computing systems. *Security and Communication Networks*, 3(6):546–564.

Artz, D. and Gil, Y. (2007). A survey of trust in computer science and the semantic web. *Web Semantics: Science, Services and Agents on the World Wide Web*, 5(2):58–71.

Azer, M. A., El-Kassas, S. M., Hassan, A. W. F., and El-Soudani, M. S. (2008). A survey on trust and reputation schemes in ad hoc networks. In *Availability, Reliability and Security, 2008. ARES 08. Third International Conference on*, pages 881–886. IEEE.

Baden, R., Bender, A., Spring, N., Bhattacharjee, B., and Starin, D. (2009). Persona: an online social network with user-defined privacy. In *ACM SIGCOMM Computer Communication Review*, volume 39-4, pages 135–146. ACM.

Beatty, P., Reay, I., Dick, S., and Miller, J. (2011). Consumer trust in e-commerce web sites: A meta-study. *ACM Computing Surveys (CSUR)*, 43(3):14.

Bevilacqua, M., Ciarapica, F., and Giacchetta, G. (2006). A fuzzy-qfd approach to supplier selection. *Journal of Purchasing and Supply Management*, 12(1):14–27.

Bhargava, B., Angin, P., Ranchal, R., Sivakumar, R., Sinclair, A., and Linderman, M. (2012). A trust-based approach for secure data dissemination in a mobile peer-to-peer network of avs. *International Journal of Next-generation Computing*, 3(1).

Boyd, D. M. and Ellison, N. B. (2007). Social network sites: Definition, history, and scholarship. *Journal of computer-mediated Communication*, 13(1):210–230.

Brunelli, M., Fedrizzi, M., and Fedrizzi, M. (2014). Fuzzy m-ary adjacency relations in social network analysis: Optimization and consensus evaluation. *Information Fusion*, 17:36–45.

Bruns, G., Fong, P. W., Siahaan, I., and Huth, M. (2012). Relationship-based access control: its expression and enforcement through hybrid logic. *CODASPY*, 12:117–124.

Buchmann, J. A. (2013). The characteristics and benefits of online social networks. In *Internet Privacy*, pages 25–41. Springer.

Buskens, V. (1998). The social structure of trust. *Social networks*, 20(3):265–289.

Cabrerizo, F. J., Al-Hmouz, R., Morfeq, A., Balamash, A. S., Martínez, M., and Herrera-Viedma, E. (2017). Soft consensus measures in group decision making using unbalanced fuzzy linguistic information. *Soft Computing*, 21(11):3037–3050.

Cabrerizo, F. J., Chiclana, F., Al-Hmouz, R., Morfeq, A., Balamash, A. S., and Herrera-Viedma, E. (2015). Fuzzy decision making and consensus: challenges. *Journal of Intelligent & Fuzzy Systems*, 29(3):1109–1118.

Carlson, C. R. and Rousselle, H. (2020). Report and repeat: Investigating facebook's hate speech removal process. *First Monday*, 25(2).

Carlsson, C. and Fullér, R. (1996). Fuzzy multiple criteria decision making: Recent developments. *Fuzzy sets and systems*, 78(2):139–153.

Carminati, B., Ferrari, E., and Perego, A. (2006). Rule-based access control for social networks. In *OTM Confederated International Conferences" On the Move to Meaningful Internet Systems"*, pages 1734–1744. Springer.

Caverlee, J., Liu, L., and Webb, S. (2008). Socialtrust: Tamper-resilient trust establishment in online communities. In *Proceedings of the 8th ACM/IEEE-CS Joint Conference on Digital Libraries*, JCDL '08, pages 104–114, New York, NY, USA. ACM.

Chen, S.-M. and Chen, Y.-C. (2002). Automatically constructing membership functions and generating fuzzy rules using genetic algorithms. *Cybernetics &Systems*, 33(8):841–862.

Cheng, Y., Park, J., and Sandhu, R. (2012). Relationship-based access control for online social networks: Beyond user-to-user relationships. In *2012 International Conference on Privacy, Security, Risk and Trust and 2012 International Confernece on Social Computing*, pages 646–655. IEEE.

Cherdantseva, Y. and Hilton, J. (2012). The evolution of information security goals from the 1960s to today. *Unpublished*.

Cherdantseva, Y. and Hilton, J. (2013). A reference model of information assurance & security. In *2013 International Conference on Availability, Reliability and Security*, pages 546–555. IEEE.

Cheung, C. M. and Lee, M. K. (2010). A theoretical model of intentional social action in online social networks. *Decision support systems*, 49(1):24–30.

Cho, S., Huh, J., and Faber, R. J. (2014). The influence of sender trust and advertiser trust on multistage effects of viral advertising. *Journal of advertising*, 43(1):100–114.

Commission, E. (2019). 2018 reform of eu data protection rules. URL:/https://ec.europa.eu/commission/sites/beta-political/files/data-protection-factsheet-changes-en.pdf/.

Coulter, K. S. and Coulter, R. A. (2002). Determinants of trust in a service provider: the moderating role of length of relationship. *Journal of services marketing*, 16(1):35–50.

Coupland, S. and John, R. (2007). Geometric type-1 and type-2 fuzzy logic systems. *IEEE Transactions on Fuzzy Systems*, 15(1):3–15.

Danny, M. N., Kogeda, O. P., and Mtsweni, J. (2016). A context-sensitive trust model for online social networking. In *Advances in Computing and Communication Engineering (ICACCE), 2016 International Conference on*, pages 314–319. IEEE.

Das, T. (2016). Intelligent techniques in decision making: A survey. *Indian Journal of Science and Technology*, 9(12).

Dasarathy, B. V. (1997). Sensor fusion potential exploitation-innovative architectures and illustrative applications. *Proceedings of the IEEE*, 85(1):24–38.

Dodig-Crnkovic, G. (2002). Scientific methods in computer science. In *Proceedings of the Conference for the Promotion of Research in IT at New Universities and at University Colleges in Sweden, Skövde, Suecia*, pages 126–130.

Dong, Y., Chen, X., and Herrera, F. (2015). Minimizing adjusted simple terms in the consensus reaching process with hesitant linguistic assessments in group decision making. *Information Sciences*, 297:95–117.

Dong, Y., Zha, Q., Zhang, H., Kou, G., Fujita, H., Chiclana, F., and Herrera-Viedma, E. (2018). Consensus reaching in social network group decision making: Research paradigms and challenges. *Knowledge-Based Systems*, 162:3–13.

Du, J., Jiang, C., Chen, K.-C., Ren, Y., and Poor, H. V. (2018). Community-structured evolutionary game for privacy protection in social networks. *IEEE Transactions on Information Forensics and Security*, 13(3):574–589.

Dunbar, R. I. (2016). Do online social media cut through the constraints that limit the size of offline social networks? *Royal Society Open Science*, 3(1):150292.

Durkheim, E. (1893). *The division of labor in society*. Simon and Schuster.

Dutta, P. and Kumaravel, A. (2016). A novel approach to trust based identification of leaders in social networks. *Indian Journal of Science and Technology*, 9(10):1–9.

Dwyer, C., Hiltz, S., and Passerini, K. (2007a). Trust and privacy concern within social networking sites: A comparison of facebook and myspace. *AMCIS 2007 proceedings*, page 339.

Dwyer, C., Hiltz, S., and Passerini, K. (2007b). Trust and privacy concern within social networking sites: A comparison of facebook and myspace. *AMCIS 2007 proceedings*, page 339.

El Marrakchi, M., Bensaid, H., and Bellafkih, M. (2015). Scoring reputation in online social networks. In *2015 10th International Conference on Intelligent Systems: Theories and Applications (SITA)*, pages 1–6. IEEE.

Elio, R., Hoover, J., Nikolaidis, I., Salavatipour, M., Stewart, L., and Wong, K. (2011). About computing science research methodology.

Ellison, N. B., Steinfield, C., and Lampe, C. (2007). The benefits of facebook "friends:" social capital and college students' use of online social network sites. *Journal of computer-mediated communication*, 12(4):1143–1168.

Fire, M., Kagan, D., Elyashar, A., and Elovici, Y. (2014). Friend or foe? fake profile identification in online social networks. *Social Network Analysis and Mining*, 4(1):194.

Fong, P. W. and Siahaan, I. (2011). Relationship-based access control policies and their policy languages. In *Proceedings of the 16th ACM symposium on Access control models and technologies*, pages 51–60. ACM.

Garton, L., Haythornthwaite, C., and Wellman, B. (1997). Studying online social networks. *Journal of computer-mediated communication*, 3(1):JCMC313.

Gates, C. (2007). Access control requirements for web 2.0 security and privacy. *IEEE Web*, 2(0).

Gibson, J. P. and Méry, D. (2018). Explicit modelling of physical measures: from event-b to java. *arXiv preprint arXiv:1805.05517*.

Golbeck, J. (2005). Web-based social networks: a survey and future directions. *Technique Report*.

Golbeck, J. (2006). Trust on the world wide web: A survey. *Foundations and Trends in Web Science*, 1 (2).

Gong, N. Z. and Wang, D. (2014). On the security of trustee-based social authentications. *arXiv preprint arXiv:1402.2699*.

Grabner-Kräuter, S. and Bitter, S. (2015). Trust in online social networks: A multifaceted perspective. In *Forum for social economics*, volume 44-1, pages 48–68. Taylor & Francis.

Hajdu, G., Minoso, Y., Lopez, R., Acosta, M., and Elleithy, A. (2019). Use of artificial neural networks to identify fake profiles. In *2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT)*, pages 1–4. IEEE.

Hamdi, S., Gancarski, A. L., Bouzeghoub, A., and Yahia, S. B. (2016). Tison: Trust inference in trust-oriented social networks. *ACM Transactions on Information Systems (TOIS)*, 34(3):1–32.

Hanneman, R. A. and Riddle, M. (2005). Introduction to social network methods.

Harel, G. and Confrey, J. (1994). *Development of Multiplicative Reasoning in the Learning of Mathematics, The*. Suny Press.

Herrera-Viedma, E., Alonso, S., Chiclana, F., and Herrera, F. (2007). A consensus model for group decision making with incomplete fuzzy preference relations. *IEEE Transactions on fuzzy Systems*, 15(5):863–877.

Herrera-Viedma, E., Cabrerizo, F. J., Chiclana, F., Wu, J., Cobo, M. J., and Konstantin, S. (2017). Consensus in group decision making and social networks. *Open Access*.

Hochbaum, D. S. and Levin, A. (2006). Methodologies and algorithms for group-rankings decision. *Management Science*, 52(9):1394–1408.

Hogg, T. and Adamic, L. (2004). Enhancing reputation mechanisms via online social networks. *EC*, 4:236–237.

Hörner, J. (2002). Reputation and competition. *American economic review*, 92(3):644–663.

Hosseini, R., Qanadli, S. D., Barman, S., Mazinani, M., Ellis, T., and Dehmeshki, J. (2012). An automatic approach for learning and tuning gaussian interval type-2 fuzzy membership functions applied to lung cad classification system. *IEEE Transactions on Fuzzy Systems*, 20(2):224–234.

Hu, H., Ahn, G.-J., and Jorgensen, J. (2011). Detecting and resolving privacy conflicts for collaborative data sharing in online social networks. In *Proceedings of the 27th Annual Computer Security Applications Conference*, pages 103–112. ACM.

Hu, H., Ahn, G.-J., and Jorgensen, J. (2012). Multiparty access control for online social networks: model and mechanisms. *IEEE Transactions on Knowledge and Data Engineering*, 25(7):1614–1627.

Hu, V. C., Kuhn, D. R., and Ferraiolo, D. F. (2015). Attribute based access control. *IEEE Computer Society*, 48(1):85–88.

Hüllermeier, E. (2015). From knowledge-based to data-driven fuzzy modeling. *Informatik-Spektrum*, 38(6):500–509.

Ilic, J., Humski, L., Pintar, D., Vranić, M., and Skocir, Z. (2016). Proof of concept for comparison and classification of online social network friends based on tie strength calculation model. In *6th interantional conference on information society and technology*.

Isdal, T., Piatek, M., Krishnamurthy, A., and Anderson, T. (2010). Privacy-preserving p2p data sharing with oneswarm. *ACM SIGCOMM Computer Communication Review*, 40(4):111–122.

Ishizaka, A. (2014). Comparison of fuzzy logic, ahp, fahp and hybrid fuzzy ahp for new supplier selection and its performance analysis. *International Journal of Integrated Supply Management*, 9(1/2):1–22.

Jamsandekar, S. S. and Mudholkar, R. R. (2014). Fuzzy classification system by self generated membership function using clustering technique. *BVICA M's International Journal of Information Technology*, 6(1):697.

Jensen, C., Davis, J., and Farnham, S. (2002). Finding others online: reputation systems for social online spaces. In *Proceedings of the SIGCHI conference on Human factors in computing systems*, pages 447–454. ACM.

Jiang, W., Wang, G., Bhuiyan, M. Z. A., and Wu, J. (2016). Understanding graph-based trust evaluation in online social networks: Methodologies and challenges. *ACM Computing Surveys (CSUR)*, 49(1):10.

Jiang, W., Wu, J., Li, F., Wang, G., and Zheng, H. (2015). Trust evaluation in online social networks using generalized network flow. *IEEE Transactions on Computers*, 65(3):952–963.

Joinson, A. N., Paine, C., Buchanan, T., and Reips, U.-D. (2008). Measuring self-disclosure online: Blurring and non-response to sensitive items in web-based surveys. *Computers in Human Behavior*, 24(5):2158–2171.

Josang, A. and Ismail, R. (2002). The beta reputation system. In *Proceedings of the 15th bled electronic commerce conference*, volume 5, pages 2502–2511.

Jøsang, A., Ismail, R., and Boyd, C. (2007). A survey of trust and reputation systems for online service provision. *Decision support systems*, 43(2):618–644.

Joseph, N. S. (2014). Collaborative data sharing in online social network resolving privacy risk and sharing loss. *IOSR-JCE) eISSN*, pages 2278–0661.

Kayes, I. and Iamnitchi, A. (2017). Privacy and security in online social networks: A survey. *Online Social Networks and Media*, 3:1–21.

Kim, Y. A. and Ahmad, M. A. (2013). Trust, distrust and lack of confidence of users in online social media-sharing communities. *Knowledge-Based Systems*, 37:438–450.

Koyuncu, M. and Yazici, A. (2005). A fuzzy knowledge-based system for intelligent retrieval. *IEEE Transactions on Fuzzy Systems*, 13(3):317–330.

Krasnova, H., Spiekermann, S., Koroleva, K., and Hildebrand, T. (2010). Online social networks: Why we disclose. *Journal of information technology*, 25(2):109–125.

Krishnan, R., Sandhu, R., and Ranganathan, K. (2007). Pei models towards scalable, usable and high-assurance information sharing. In *Proceedings of the 12th ACM symposium on Access control models and technologies*, pages 145–150. ACM.

Krohn, M., Yip, A., Brodsky, M., Cliffer, N., Kaashoek, M. F., Kohler, E., and Morris, R. (2007). Information flow control for standard os abstractions. *ACM SIGOPS Operating Systems Review*, 41(6):321–334.

Labella, Á., Estrella, F. J., and Martínez, L. (2017). Afryca 2.0: an improved analysis framework for consensus reaching processes. *Progress in Artificial Intelligence*, 6(2):181–194.

Ledbetter, A. M., Mazer, J. P., DeGroot, J. M., Meyer, K. R., Mao, Y., and Swafford, B. (2011). Attitudes toward online social connection and self-disclosure as predictors of facebook communication and relational closeness. *Communication Research*, 38(1):27–53.

Leijnse, A. and Hassanizadeh, S. M. (1995). Model definition and model validation. In *International Journal of Rock Mechanics and Mining Sciences and Geomechanics Abstracts*, volume 5-32, page 209A.

Li, F., Pieńkowski, D., van Moorsel, A., and Smith, C. (2012). A holistic framework for trust in online transactions. *International Journal of Management Reviews*, 14(1):85–103.

Li, L., Scaglione, A., Swami, A., and Zhao, Q. (2013). Consensus, polarization and clustering of opinions in social networks. *IEEE Journal on Selected Areas in Communications*, 31(6):1072–1083.

Li, M., Wang, X., Gao, K., and Zhang, S. (2017). A survey on information diffusion in online social networks: Models and methods. *Information*, 8(4):118.

Li, Y., Li, Y., Yan, Q., and Deng, R. H. (2015). Privacy leakage analysis in online social networks. *Computers & Security*, 49:239–254.

Li, Y.-M., Chen, H.-M., Liou, J.-H., and Lin, L.-F. (2014). Creating social intelligence for product portfolio design. *Decision Support Systems*, 66:123–134.

Li, Y.-M. and Lai, C.-Y. (2014). A social appraisal mechanism for online purchase decision support in the micro-blogosphere. *Decision Support Systems*, 59:190–205.

Liang, H., Dong, Y., and Li, C. (2016). Dynamics of uncertain opinion formation: An agent-based simulation. *Journal of Artificial Societies and Social Simulation*, 19(4).

Liang, Q., Liao, X., and Liu, J. (2017). A social ties-based approach for group decision-making problems with incomplete additive preference relations. *Knowledge-Based Systems*, 119:68–86.

Liang, X., Zhang, K., Shen, X., and Lin, X. (2014). Security and privacy in mobile social networks: challenges and solutions. *IEEE Wireless Communications*, 21(1):33–41.

Liben-Nowell, D. and Kleinberg, J. (2008). Tracing information flow on a global scale using internet chain-letter data. *Proceedings of the national academy of sciences*, 105(12):4633–4638.

Liu, G. (2013). *Trust management in online social networks*. Macquarie University, Faculty of Science, Department of Computing.

Liu, H., Cocea, M., and Ding, W. (2018). Multi-task learning for intelligent data processing in granular computing context. *Granular Computing*, 3(3):257–273.

Lu, Y. and Li, S. (2020). From data flows to privacy issues: a user-centric semantic model for representing and discovering privacy issues. In *Proceedings of 53rd Hawaii International Conference on System Sciences*.

Lu, Y., Wang, W., Bhargava, B., and Xu, D. (2006). Trust-based privacy preservation for peer-to-peer data sharing. *IEEE Transactions on Systems, Man, and Cybernetics-Part A: Systems and Humans*, 36(3):498–502.

Majumder, M. (2015). Multi criteria decision making. In *Impact of urbanization on water shortage in face of climatic aberrations*, pages 35–47. Springer.

Mamdani, E. and Assilian, S. (1999). An experiment in linguistic synthesis with a fuzzy logic controller. *International journal of human-computer studies*, 51(2):135–147.

Marin, A. and Wellman, B. (2011). Social network analysis: An introduction. *The SAGE handbook of social network analysis*, 11.

McGoldrick, D. (2013). The Limits of Freedom of Expression on Facebook and Social Networking Sites: A UK Perspective. *Human Rights Law Review*, 13(1):125–151.

McLeod, A. and Pippin, S. E. (2009). Security and privacy trust in e-government: Understanding system and relationship trust antecedents. In *2009 42nd Hawaii International Conference on System Sciences*, pages 1–10. IEEE.

Mehra, A., Dixon, A. L., Brass, D. J., and Robertson, B. (2006). The social network ties of group leaders: Implications for group performance and leader reputation. *Organization science*, 17(1):64–79.

Momani, M. and Challa, S. (2010). Survey of trust models in different network domains. *arXiv preprint arXiv:1010.0168*.

Moreno, J. L. (1934). Who shall survive?: A new approach to the problem of human interrelations. *American Psychological Association*.

MySQL, A. (2001). Mysql.

Nielson, H. R. and Nielson, F. (2017). Content dependent information flow control. *Journal of Logical and Algebraic Methods in Programming*, 87:6–32.

Nosko, A., Wood, E., and Molema, S. (2010). All about me: Disclosure in online social networking profiles: The case of facebook. *Computers in human behavior*, 26(3):406–418.

Ohst, D., Welle, M., and Kelter, U. (2003). Differences between versions of uml diagrams. In *Proceedings of the 9th European software engineering conference held jointly with 11th ACM SIGSOFT international symposium on Foundations of software engineering*, pages 227–236.

Ojo, A. K. (2019). Improved model for detecting fake profiles in online social network: A case study of twitter. *Journal of Advances in Mathematics and Computer Science*, pages 1–17.

Olsina, L. and Becker, P. (2018). Linking business and information need goals with functional and non-functional requirements. In *CIbSE*, pages 381–394.

Paradesi, S., Doshi, P., and Swaika, S. (2009). Integrating behavioral trust in web service compositions. In *2009 IEEE International Conference on Web Services*, pages 453–460. IEEE.

Parsons, T. (1937). The structure of. *Social Action*, 491.

Paul, S. A., Hong, L., and Chi, E. H. (2012). Who is authoritative? understanding reputation mechanisms in quora. *arXiv preprint arXiv:1204.3724*.

Pérez, L. G., Mata, F., Chiclana, F., Kou, G., and Herrera-Viedma, E. (2016). Modelling influence in group decision making. *Soft Computing*, 20(4):1653–1665.

Petkos, G., Papadopoulos, S., and Kompatsiaris, Y. (2015). Pscore: a framework for enhancing privacy awareness in online social networks. In *2015 10th International Conference on Availability, Reliability and Security*, pages 592–600. IEEE.

Podobnik, V., Striga, D., Jandras, A., and Lovrek, I. (2012). How to calculate trust between social network users? In *SoftCOM 2012, 20th International Conference on Software, Telecommunications and Computer Networks*, pages 1–6. IEEE.

Poppo, L., Zhou, K. Z., and Li, J. J. (2016). When can you trust? "trust" calculative trust, relational trust, and supplier performance. *Strategic Management Journal*, 37(4):724–741.

Prell, C. (2012). *Social network analysis: History, theory and methodology*. Sage.

Proudfoot, J. G., Wilson, D., Valacich, J. S., and Byrd, M. D. (2018). Saving face on facebook: Privacy concerns, social benefits, and impression management. *Behaviour & Information Technology*, 37(1):16–37.

Puthal, D. (2018). Lattice-modeled information flow control of big sensing data streams for smart health application. *IEEE Internet of Things Journal*, 6(2):1312–1320.

Qian, G. and Xu, Z.-S. (2006). Extended iowa operator and its application to group decision making with linguistic preference information. In *2006 International Conference on Machine Learning and Cybernetics*, pages 1662–1666. IEEE.

Quora (2019). What does facebook mean by ”content not available” when i click on a user’s name? https://www.quora.com/What-does-Facebook-mean-by-content-not-available-when-I-click-on-a-users-name.

Rahman, M. A., Mezhuyev, V., Bhuiyan, M. Z. A., Sadat, S. N., Zakaria, S. A. B., and Refat, N. (2018). Reliable decision making of accepting friend request on online social networks. *IEEE Access*, 6:9484–9491.

Rathore, N. C. and Tripathy, S. (2017). A trust-based collaborative access control model with policy aggregation for online social networks. *Social Network Analysis and Mining*, 7(1):7.

Recio-García, J. A., Quijano, L., and Díaz-Agudo, B. (2013). Including social factors in an argumentative model for group decision support systems. *Decision Support Systems*, 56:48–55.

Richards, N. and Hartzog, W. (2015). Taking trust seriously in privacy law. *Stan. Tech. L. Rev.*, 19:431.

Riedl, C., Köbler, F., Goswami, S., and Krcmar, H. (2013). Tweeting to feel connected: A model for social connectedness in online social networks. *International Journal of Human-Computer Interaction*, 29(10):670–687.

Rivera, V., Cataño, N., Wahls, T., and Rueda, C. (2017). Code generation for event-b. *International Journal on Software Tools for Technology Transfer*, 19(1):31–52.

Ross, T. J. (2005). *Fuzzy logic with engineering applications*. John Wiley & Sons.

Roubens, M. (1997). Fuzzy sets and decision analysis. *Fuzzy sets and systems*, 90(2):199–206.

Ruohomaa, S., Kutvonen, L., and Koutrouli, E. (2007). Reputation management survey. In *The Second International Conference on Availability, Reliability and Security (ARES'07)*, pages 103–111. IEEE.

Sabatini, F. and Sarracino, F. (2019). Online social networks and trust. *Social Indicators Research*, 142(1):229–260.

Samonas, S. and Coss, D. (2014). The cia strikes back: Redefining confidentiality, integrity and availability in security. *Journal of Information System Security*, 10(3).

Sanayei, A., Mousavi, S. F., and Yazdankhah, A. (2010). Group decision making process for supplier selection with vikor under fuzzy environment. *Expert Systems with Applications*, 37(1):24–30.

Sargent, R. G. (2000). Verification, validation and accreditation of simulation models. In *2000 Winter Simulation Conference Proceedings (Cat. No. 00CH37165)*, volume 1, pages 50–59. IEEE.

Sargent, R. G. (2010). Verification and validation of simulation models. In *Proceedings of the 2010 winter simulation conference*, pages 166–183. IEEE.

Sattarova Feruza, Y. and Kim, T.-h. (2007). It security review: Privacy, protection, access control, assurance and system security. *International journal of multimedia and ubiquitous engineering*, 2(2):17–32.

Scheidt, N., Akkuzu, G., and Adda, M. (2020). Making decision on sharing forensic data with the fuzzy logic approach. In *IEEE*. IEEE.

Schweitzer, F., Mavrodiev, P., Seufert, A. M., and Garcia, D. (2019). Modeling user reputation in online social networks: The role of costs, benefits, and reciprocity. *arXiv preprint arXiv:1909.04591*.

Sherchan, W., Nepal, S., and Paris, C. (2013). A survey of trust in social networks. *ACM Computing Surveys (CSUR)*, 45(4):47.

Shin, D.-H. (2010). The effects of trust, security and privacy in social networking: A security-based approach to understand the pattern of adoption. *Interacting with computers*, 22(5):428–438.

Siddula, M., Cai, Z., and Miao, D. (2018). Privacy preserving online social networks using enhanced equicardinal clustering. In *2018 IEEE 37th International Performance Computing and Communications Conference (IPCCC)*, pages 1–8. IEEE.

Smets, P. and Magrez, P. (1987). Implication in fuzzy logic. *International Journal of Approximate Reasoning*, 1(4):327–347.

Social, W. A., Hootsuite, and DataReportal (2019). Most popular social networks worldwide as of october 2019, ranked by number of active users (in millions) [graph].

Squicciarini, A. C., Shehab, M., and Paci, F. (2009). Collective privacy management in social networks. In *Proceedings of the 18th international conference on World wide web*, pages 521–530. ACM.

Squicciarini, A. C., Shehab, M., and Wede, J. (2010). Privacy policies for shared content in social network sites. *The VLDB Journal*, 19(6):777–796.

Such, J. M. and Criado, N. (2018). Multiparty privacy in social media. *Commun. ACM*, 61(8):74–81.

Such, J. M., Porter, J., Preibusch, S., and Joinson, A. (2017). Photo privacy conflicts in social media: A large-scale empirical study. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, pages 3821–3832. ACM.

Sun, J., Zhu, X., and Fang, Y. (2010). A privacy-preserving scheme for online social networks with efficient revocation. In *2010 Proceedings IEEE INFOCOM*, pages 1–9. IEEE.

Suvitha.D (2014). Mechanisms of multiparty access control in online social network. *International Journal of Recent Development in Engineering and Technology*, 2, (3).

Takalkar, V. and Mahalle, P. N. (2018). Trust-based access control in multi-role environment of online social networks. *Wireless Personal Communications*, 100(2):391–399.

Talja, S. and Hansen, P. (2006). Information sharing. In *New directions in human information behavior*, pages 113–134. Springer.

Thirumalai, C. and Senthilkumar, M. (2017). An assessment framework of intuitionistic fuzzy network for c2b decision making. In *2017 4th International Conference on Electronics and Communication Systems (ICECS)*, pages 164–167. IEEE.

Tindale, R. S. and Winget, J. R. (2019). Group decision-making. In *Oxford Research Encyclopedia of Psychology*. Oxford Research Encyclopedias.

Tong, R. M. and Bonissone, P. P. (1980). A linguistic approach to decisionmaking with fuzzy sets. *IEEE Transactions on Systems, Man, and Cybernetics*, 10(11):716–723.

Tönnies, F. (1887). Community and society. *The urban sociology reader*, 13.

Ulusoy, O. (2018). Collaborative privacy management in online social networks. In *Proceedings of the 17th International Conference on Autonomous Agents and MultiAgent Systems*, pages 1788–1790. International Foundation for Autonomous Agents and Multiagent Systems.

Urena, R., Kou, G., Dong, Y., Chiclana, F., and Herrera-Viedma, E. (2019). A review on trust propagation and opinion dynamics in social networks and group decision making frameworks. *Information Sciences*, 478:461–475.

Van Leekwijck, W. and Kerre, E. E. (1999). Defuzzification: criteria and classification. *Fuzzy sets and systems*, 108(2):159–178.

Vartiainen, P. (2002). On the principles of comparative evaluation. *Evaluation*, 8(3):359–371.

Wang, G. and Wu, J. (2011). Multi-dimensional evidence-based trust management with multi-trusted paths. *Future Generation Computer Systems*, 27(5):529–538.

Wang, T. and Lu, Y. (2010). Determinants of trust in e-government. In *2010 International Conference on Computational Intelligence and Software Engineering*, pages 1–4. IEEE.

Wang, T.-C. and Chang, T.-H. (2007). Application of topsis in evaluating initial training aircraft under a fuzzy environment. *Expert Systems with Applications*, 33(4):870–880.

Wang, Y., Norcie, G., Komanduri, S., Acquisti, A., Leon, P. G., and Cranor, L. F. (2011). " i regretted the minute i pressed share" a qualitative study of regrets on facebook. In *Proceedings of the seventh symposium on usable privacy and security*, pages 1–16.

Wang, Y. and Vassileva, J. (2007). A review on trust and reputation for web service selection. In *Distributed computing systems workshops, 2007. ICDCSW'07. 27th International Conference on*, pages 25–25. IEEE.

Wasko, M. M., Faraj, S., et al. (2005). Why should i share? examining social capital and knowledge contribution in electronic networks of practice. *MIS quarterly*, 29(1):35–57.

Wei, G. (2019). 2-tuple intuitionistic fuzzy linguistic aggregation operators in multiple attribute decision making. *Iranian Journal of Fuzzy Systems*, 16(4):159–174.

Wishart, R., Corapi, D., Marinovic, S., and Sloman, M. (2010). Collaborative privacy policy authoring in a social networking context. In *Policies for distributed systems and networks (POLICY), 2010 IEEE international symposium on*, pages 1–8. IEEE.

Wu, J., Chiclana, F., Fujita, H., and Herrera-Viedma, E. (2017). A visual interaction consensus model for social network group decision making with trust propagation. *Knowledge-Based Systems*, 122:39–50.

Wu, J., Chiclana, F., and Herrera-Viedma, E. (2015a). Trust based consensus model for social network in an incomplete linguistic information context. *Applied Soft Computing*, 35:827–839.

Wu, J., Dai, L., Chiclana, F., Fujita, H., and Herrera-Viedma, E. (2018). A minimum adjustment cost feedback mechanism based consensus model for group decision making under social network with distributed linguistic trust. *Information Fusion*, 41:232–242.

Wu, J., Liu, Y., and Liang, C. (2015b). A consensus-and harmony-based feedback mechanism for multiple attribute group decision making with correlated intuitionistic fuzzy sets. *International Transactions in Operational Research*, 22(6):1033–1054.

Xiang, R., Neville, J., and Rogati, M. (2010). Modeling relationship strength in online social networks. In *Proceedings of the 19th international conference on World wide web*, pages 981–990. ACM.

Xu, L., Bao, T., Zhu, L., and Zhang, Y. (2018). Trust-based privacy-preserving photo sharing in online social networks. *IEEE Transactions on Multimedia*, 21(3):591–602.

Xu, L., Jiang, C., He, N., Han, Z., and Benslimane, A. (2019). Trust-based collaborative privacy management in online social networks. *IEEE Transactions on Information Forensics and Security*, 14(1):48–60.

Xu, S., Li, X., Parker, T. P., and Wang, X. (2011). Exploiting trust-based social networks for distributed protection of sensitive data. *IEEE Transactions on Information Forensics and Security*, 6(1):39–52.

Xu, Z. (2005). Deviation measures of linguistic preference relations in group decision making. *Omega*, 33(3):249–254.

Xu, Z. (2006). Induced uncertain linguistic owa operators applied to group decision making. *Information fusion*, 7(2):231–238.

Yadav, A., Chakraverty, S., and Sibal, R. (2019). A framework for classifying trust for online systems. *World Wide Web*, 22(4):1499–1521.

Yadav, H. B., Kumar, S., Kumar, Y., and Yadav, D. K. (2018). A fuzzy logic based approach for decision making. *Journal of Intelligent & Fuzzy Systems*, 35(2)(Preprint):1–9.

Yager, R. R. (1988). On ordered weighted averaging aggregation operators in multicriteria decisionmaking. *IEEE Transactions on systems, Man, and Cybernetics*, 18(1):183–190.

Yager, R. R. (2018). Decision making under measure-based granular uncertainty. *Granular Computing*, pages 1–9.

Yager, R. R. and Filev, D. P. (1999). Induced ordered weighted averaging operators. *IEEE Transactions on Systems, Man, and Cybernetics, Part B (Cybernetics)*, 29(2):141–150.

Yang, L. and Tan, B. C. (2012). Self-disclosure on online social networks: motives, context feature, and media capabilities. *AIS eLibrary*.

Yu, X. and Wang, Z. (2010). A enhanced trust model based on social network and online behavior analysis for recommendation. In *Computational Intelligence and Software Engineering (CiSE), 2010 International Conference on*, pages 1–4. IEEE.

Yuan, D., Miao, Y., Gong, N. Z., Yang, Z., Li, Q., Song, D., Wang, Q., and Liang, X. (2019). Detecting fake accounts in online social networks at the time of registrations. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, pages 1423–1438.

Zadeh, L. A. (2008). Is there a need for fuzzy logic? *Information sciences*, 178(13):2751–2779.

Zdancewic, S. and Myers, A. C. (2001). Secure information flow and cps. In *European Symposium on Programming*, pages 46–61. Springer.

Zeng, S. and Su, W. (2011). Intuitionistic fuzzy ordered weighted distance operator. *Knowledge-Based Systems*, 24(8):1224–1232.

Zhang, D. and Guo, G. (2014). A comparison of online social networks and real-life social networks: a study of sina microblogging. *Mathematical Problems in Engineering*, 2014.

Zhang, Z. and Wang, K. (2013). A trust model for multimedia social networks. *Social Network Analysis and Mining*, 3(4):969–979.

Zhu, Z. (2013). Discovering the influential users oriented to viral marketing based on online social networks. *Physica A: Statistical Mechanics and its Applications*, 392(16):3459–3469.

Appendix A

Appendices

A.1 Appendix A: Generating Membership Functions Using Clustering Technique

We give more explanation about fuzzy-logic decision system. In Chapter 4, we have defined the fuzzy-logic based decision making for this thesis. In this chapter, the defined fuzzy-logic based decision system has two inputs and one output, data sensitivity and confidence in co-owned data targeted group are inputs and decision is output variable. As it is mentioned in Chapter 4, fuzzy decision is based on the fuzzy logic in which the decision values are ranged from 0 to 1 rather than binary values (0 or 1). A fuzzy set is defined (U, μ) in which U represents the universe set of elements and μ represents the membership function with its membership degrees; $x \in U \rightarrow \mu(x) \in [0,1]$.

A fuzzy system mainly is composed of fuzzification, fuzzy inference, and defuzzification. In fuzzification phase, each linguistic term is mapped to a continuous attribute into a membership degree value. In the fuzzy inference stage, rules are defined with the linguistic

terms of input variables and linguistic term of output variable. For example;

· **x is A:** antecedent

· **Rule:** If x is A then y is B

· **y is B:** consequent

In given fuzzy rule x is A and y is B can be true to a degree, instead being entirely true or false Koyuncu and Yazici (2005), the antecedent may be composed of one condition or more than one condition by *AND* and *OR* logical operators. For example;

· **Rule 1:** If x_1 is A_{11} AND x_2 is A_{21} THEN decision= D_1

· **Rule 2:** If x_1 is A_{11} OR (x_1 is A_{12} AND x_2 is A_{22}) THEN decision=D_2

.

.

· **Rule m:** If x_1 is A_{1m} AND x_2 is A_{nm} THEN decision=D_k

A_{nm} is and indication of a linguistic term in which n represents A's input attribute and m represent the rule index. D_k represents a decision label, k is the decision index.

Different defuzzification methods were introduced by Ross in 2014 Ross (2005) such as the centroid method, the mean-max membership, the maximum membership principle, and the centre of sums. We adopt the centre of sums method in our work which is the most commonly used defuzzification technique.

$$x^* = \frac{\sum i = 1^N x_i . \sum k = 1^n \mu_{Ak}(x_i)}{\sum i = 1^N x_i + \sum k = 1^n \mu_{Ak}(x_i)} \tag{A.1}$$

Equation A.1 is the representation of the centre of sums defuzzification method in which n is the number of fuzzy sets, N is the number of fuzzy variables, and μ_{Ak} is the membership function for the k-th fuzzy set. The defuzzified value x^* is as follows;

$$x^* = \frac{\sum i = 1^k A_i \times \overline{\mathrm{x_l}}}{\sum i = 1^k A_i} \tag{A.2}$$

A_i indicates the firing area of i_h^t rules, k represents the total number of rules fired out, and $\overline{\mathrm{x_l}}$ is the centre of area.

Based on fuzzy systems and data, the membership functions' shapes are chosen. There are various shapes of membership functions in fuzzy set, such as triangle, trapezoid, and rectangle. It can be clearly seen that trapezoid comprises triangle and rectangular membership functions. For example, in Figure A.1 if a=b and c=d, then the shape of membership function would become rectangular. On the other hand, if b=c, then the shape would become triangle.

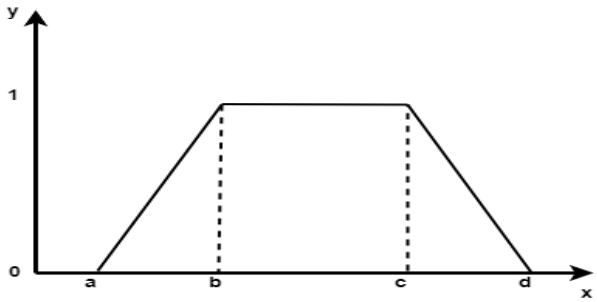

Figure A.1: Trapezoid Membership Function

The membership function of the trapezoidal fuzzy set is defined by a function x, and essentially depends on four parameters a,b,c,d as given below.

$$f_T(x) = \begin{cases} 0, & x \leq a \text{ or } x \geq d \quad \text{(A.3)} \\ \dfrac{x-a}{b-a}, & a \leq x \leq b \quad \text{(A.4)} \\ 1, & b \leq x \leq c \quad \text{(A.5)} \\ \dfrac{d-x}{d-c}, & c \leq x \leq d \quad \text{(A.6)} \end{cases}$$

There are two ways to define membership functions, either expert knowledge can be used to define membership functions Mamdani and Assilian (1999) or data can be used to find the membership functions with the machine learning techniques Hosseini et al. (2012), Jamsandekar and Mudholkar (2014).

The clustering method is used to group a set of similar objects into the same group (cluster). We use Fuzzy C-Means clustering method to define fuzzy input variables' membership functions' values. We now explain the steps of creating membership functions for input and output variables with clustering. For input variables membership functions; *Fuzzy C-Means* algorithm is used to create clusters on the input variables' values and the output variable values. Jamsandekar and Mudholkar (2014) have applied a clustering method for generating membership functions for data driven membership function generation, we used the same method with *Fuzzy C-Means* algorithm. In order to create membership functions for input and output variables, we take following steps;

- C-means Clustering method is used to form clusters on input variable data for each value to form three clusters. Three cluster central points are formed to the center of three fuzzy triangular membership functions.

- Each cluster's maximum and minimum values are determined with the determination of two vertexes of each triangular fuzzy membership function. Then each

cluster's maximum value is increased by 10% for defining the next vertex. We then increased the minimum value for each cluster by 10% for forming the next point of membership functions.

- As it is mentioned previously, we use trapezoidal membership function in this thesis fuzzy system (see Figure A.1). Point c is calculated by 10% difference minimum of first triangular membership function by clustering itself, we then increased the first triangular membership function's minimum value 15% for forming d point in the figure. This step is taken for defining the left extreme trapezoidal membership functions' each point. In order to define the right extreme trapezoidal membership functions, a point is formed by calculating 10% of obtained maximum value. The next step is to form point b in the figure, 5% difference of the maximum value is obtained for the next triangular membership cluster with itself.

Table A.1 and Table A.2 represent each cluster's minimum and maximum values for input variables. Sensitivity and confidence are input variables for the fuzzy system, maximum and minimum values for these input variables are computed.

Table A.1: Max and Min Value of Sensitivity

Sensitivity Cluster	Minimum Value	Maximum Value
$Cluster_1$	0.27	0.48
$Cluster_2$	0.51	0.64
$Cluster_3$	0.67	0.89

Table A.2: Max and Min Value of Confidence

Confidence Cluster	Minimum Value	Maximum Value
$Cluster_1$	0.84	0.59
$Cluster_2$	0.56	0.46
$Cluster_3$	0.39	0.23

Left and right vertexes of input variables' membership functions are given in Table A.3 and Table A.4. These tables' values are used to calculate the membership functions.

Table A.3: Left and Right Vertex Point of Sensitivity

Membership Function	Right Vertex	Left Vertex
Low	0.39	0.18
Medium	0.37	0.59
High	0.9	0.5

Table A.4: Left and Right Vertex Point of Confidence

Membership Function	Right Vertex	Left Vertex
Low	0.39	0.18
Medium	0.37	0.59
High	0.9	0.5

A.2 Appendix B: *Trusty* System's User Manuel

This section presents the *Trusty* web-site characteristic behaviours which involve actions that a user can do. In order to show all activities in *Trusty*, we have created two test user accounts. The test accounts have been used for testing not only *Trusty* but also the implementation of the developed models.

- Visit `http://www.trusty.gen.tr/`

  Figure A.2 presents the *Trusty* social network main page which is categorised into three different sections namely *Create an account*, *About Trusty*, and *log in*. Users need to provide first name, last name, email address, and password in order to create an account on the *Trusty*. The criteria for the password is that the password should include at least 8 characters. *About Trusty* gives brief information about the online social network.

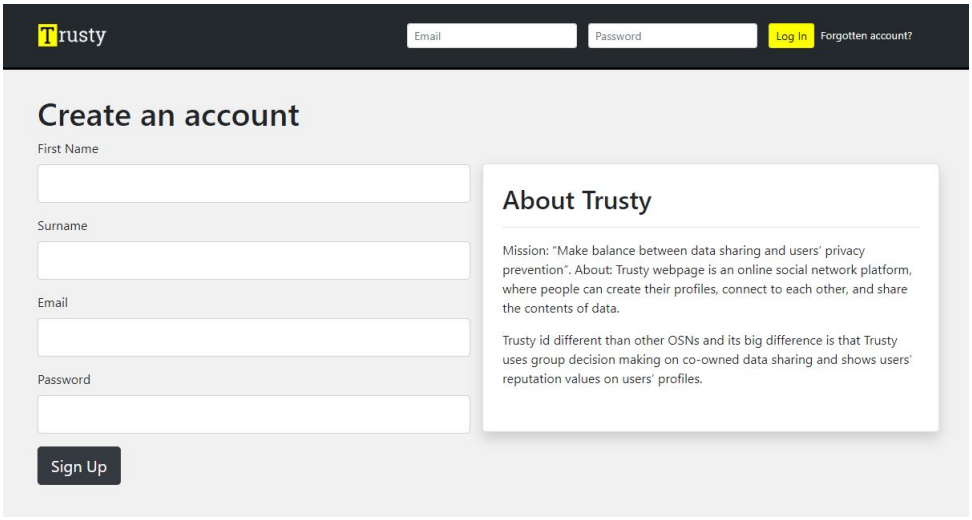

Figure A.2: *Trusty* Homepage

- Once the required information is completed for signing an account, the *Trusty* allows users to login. Each user is given a profile page in which users can see their starting reputation value and their personal information which they saved when they set up their accounts. Each user can upload a profile photo, which will be available to the *Trusty* users. Users can find friends on the *Trusty* and can share contents of data such as videos, texts, and photos.

  There are three accounts on *Trusty*, which are named *useruser*, *user1user1*, and *user2user2*. These account are used to explain *How users can interact to each other on Trusty?* and *How the developed models are used on Trusty?* Figure A.3 presents one of test accounts' profile page. As it is seen, users are allowed to upload either photos or create text messages for sharing. They can also specify the people who can access the shared data in the section "*Who should see this?*".

- Users can tag friends on a post. Once they tag a friend on a content of data, the content of data is considered as co-owned data on Trusty. Trusty notifies tagged user or users and waits for their choices.

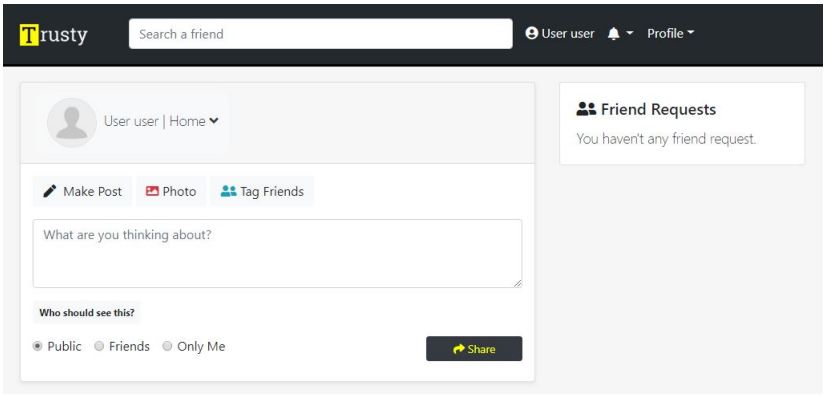

Figure A.3: A Profile Page on Trusty

Figure A.4 shows the steps for tagging a user on a content of data on *Trusty*. First step is to fill the part for making a post. In Figure A.4, making post part is numbered with number *1*. Other users (*i.e. co-owners*), who are considered related to the content of data, are tagged with the searching bar see *2* in Figure A.4. The next part is to choose the targeted group for the content. There are three options *Public, Friends, OnlyMe*. Once the content of data is uploaded, users (co-owners) are tagged, and the targeted group is chosen, user finally can press the notification button (see Figure A.4 *Notify* section).

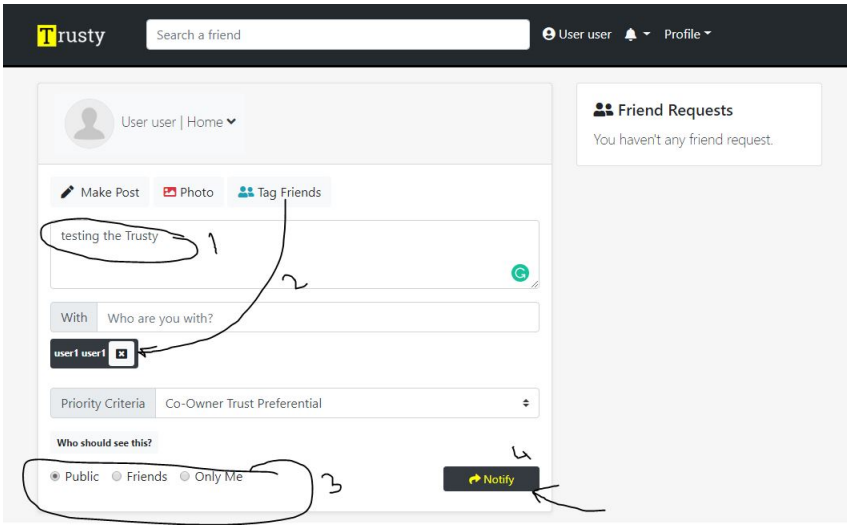

Figure A.4: Tagging Friends

Trusty notifies the tagged users, the content is not allowed to post until tagged users (co-owners) make their choices. User is given a notification which is *Waiting for co-owners* (see Figure A.5).

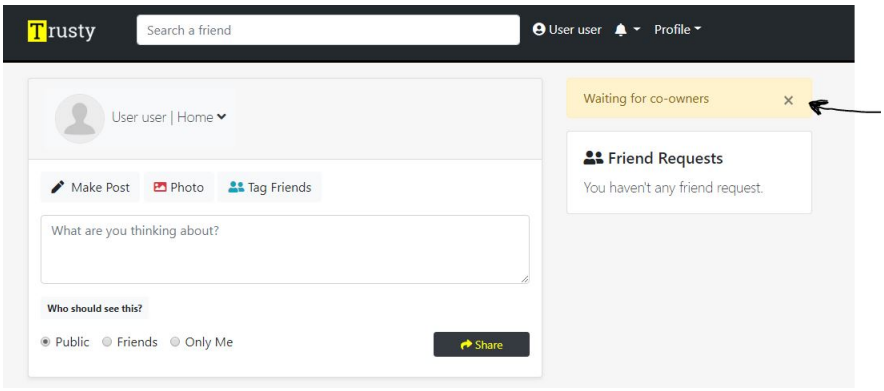

Figure A.5: Waiting for Tagged Friend's Choices

- *Trusty* notifies the tagged user (co-owners). In the tagged user's page, a notification appears $User_i$ *tagged you in a post.* Figure A.6 presents the notification on the tagged user's account.

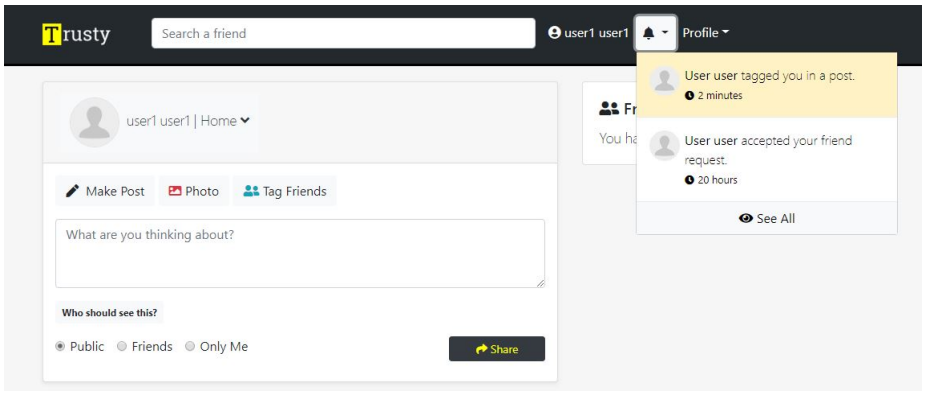

Figure A.6: Notification on Tagged User's Account

- When the user clicks on the notification, the choices are brought to the user. Figure A.7 presents the page that is given to co-owner in order to give their concerns on the data security features and alternative choices for choosing sharing options.

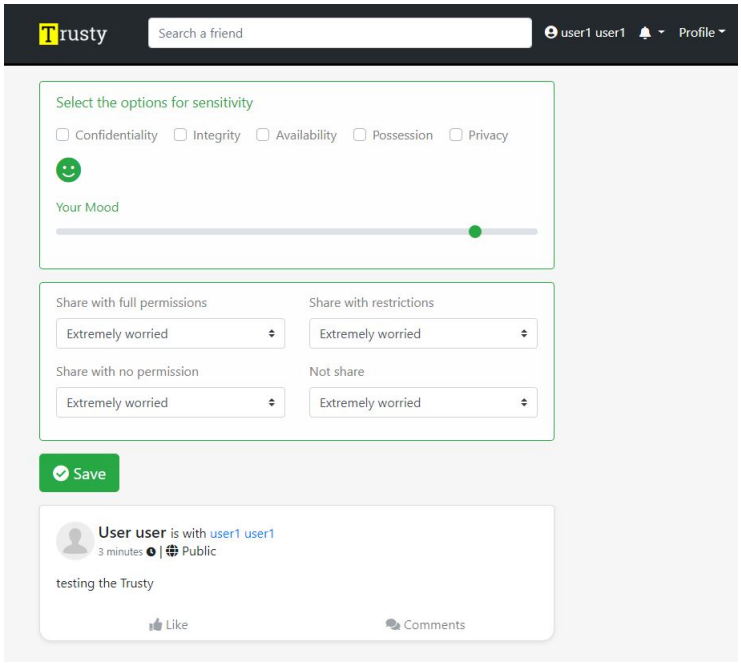

Figure A.7: Page for Selecting Choices

- Figure A.8 shows which part is used for what. The data sensitivity value, which is given in Chapter 5, is calculated with the user's choices on CIAPP features. The consensus-reached decision making choices, mentioned in Chapter 6, are given in the figure.

- User is allowed to choose the mood, which affects the calculation of Trust values. The mood has three different cases. Figure A.9 gives the mood cases on the scroll bar on the *Trusty*. As it is seen, there are three moods on the *Trusty* namely *Unhappy*, *Neutral*, *Happy*.

- Choices for consensus-based group decision making is also given on the same page. Representation of the alternatives, which are given in Chapter 6 are shown in the following figure.

- The *Trusty* makes a final notification for the user. The notification shows that the user made selections for the calculations. The following figure indicates the final

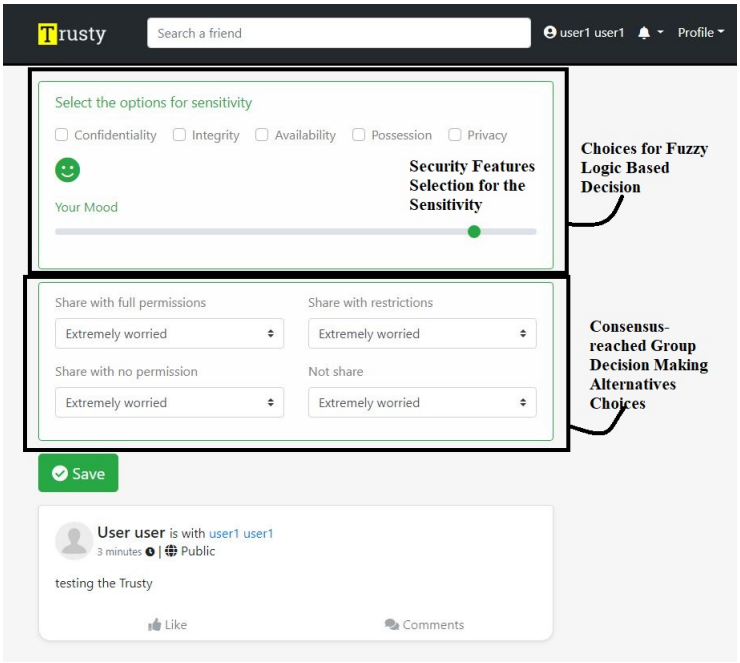

Figure A.8: Sections for Fuzzy Logic Decision and Group Decision Making

notification.

- Finally, the *Trusty* makes a notification to the user (*i.e. owner*). The notification is to inform the owner, the co-owners' decision and the fuzzy decision. Figure A.12 shows co-owner's (*user1 user1*) decision to the owner (*user user*). Figure A.13 presents the group's decision (*co-owners' decision*) with details of trust values for each decision maker (*i.e. co-owner*). This notification gives what is trust-loss/ trust-gain for each user in the group.

- The future flow of co-owned data control has been introduced in Chapter 7. Given refined machine is used for the implementation because it comprises of the specifications for control flow. The control flow should be only activated when data targeted group is specified, for example, if the targeted group is chosen *public*, then the controlling does not need to be activated. If the data targeted group is specified, then the flow control can be activated on shared data. Figure A.14 presents the

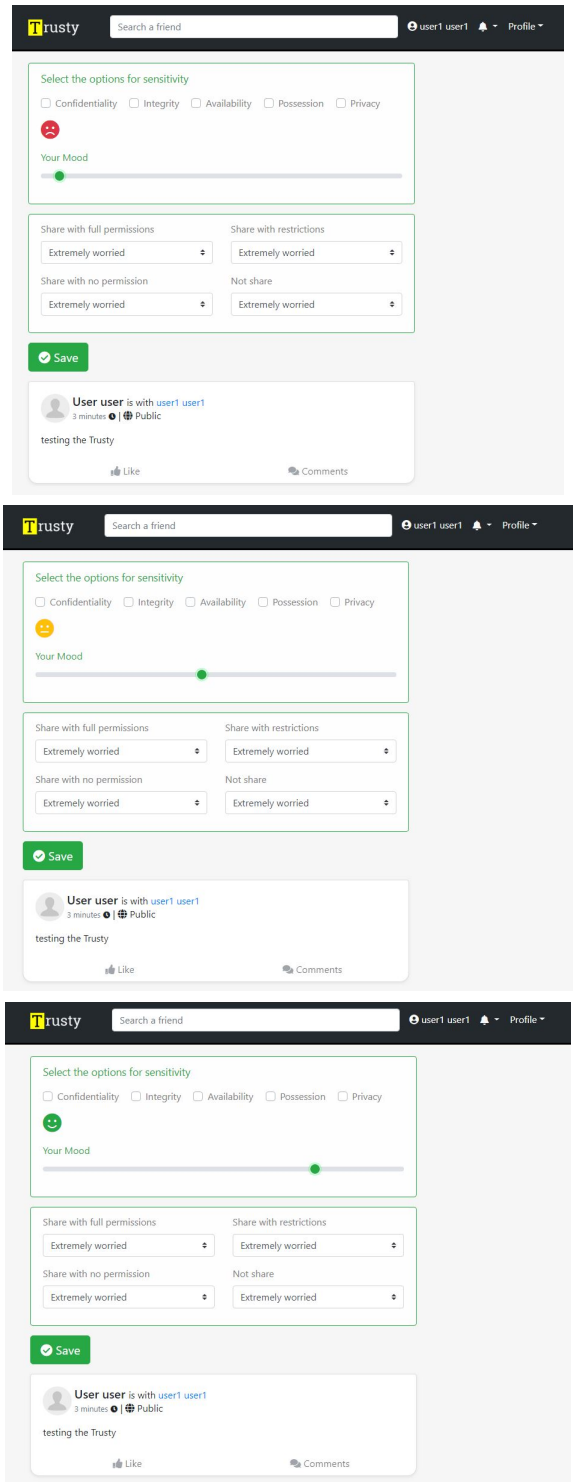

Figure A.9: Mood Unhappy, Mood Neutral, and Mood Happy

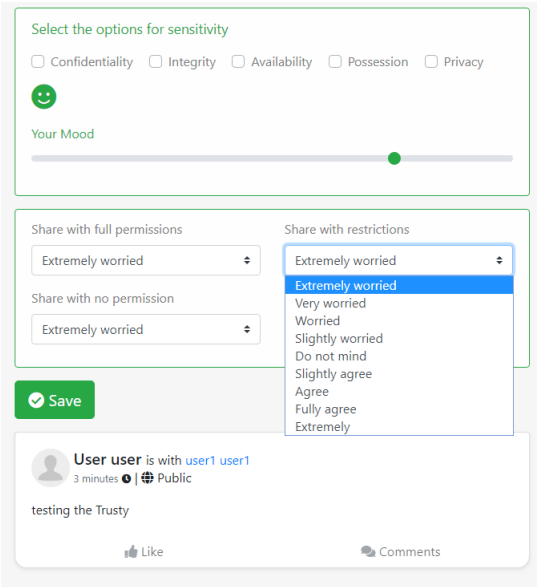

Figure A.10: Alternatives for Consensus-based Group Decision

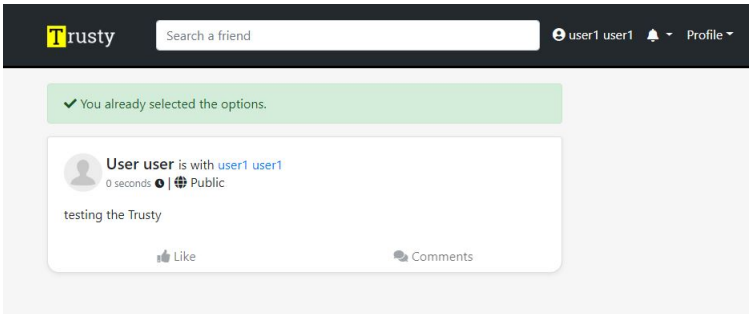

Figure A.11: Final Notification for the User (co-owner)

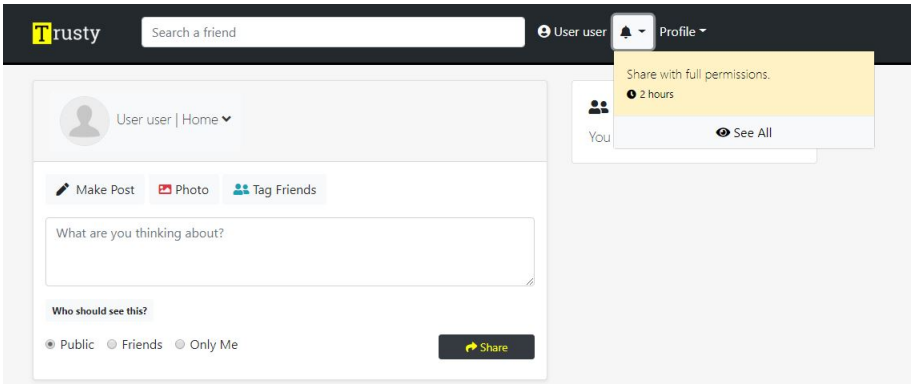

Figure A.12: The Notification for the User (owner)

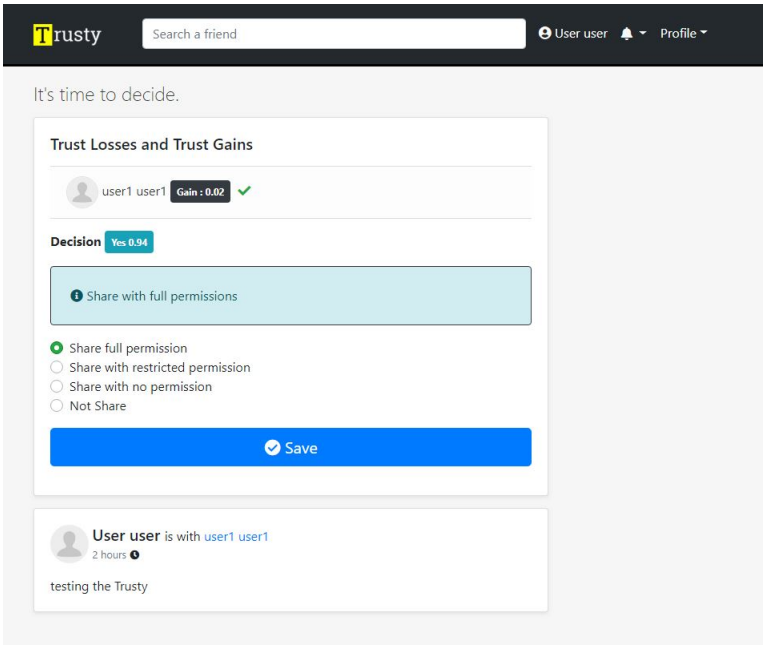

Figure A.13: The Final page for the User (owner)

activation of the flow control with *Control flow of data* button.

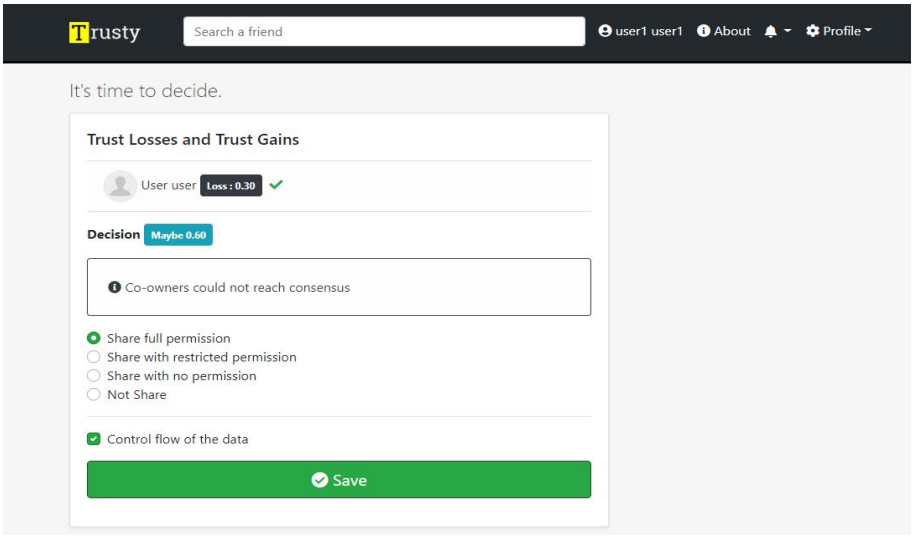

Figure A.14: The Final page for the User (owner) with control flow Activation

A.2.1 Trusty Dataset

The *Trusty* network is an OSNs in which any person can have an account by providing the required information namely, first name, surname, email address, and password. The *Trusty* social network has been introduced in different places such as *bis conference 2019*, *SNAMS conference 2019*, and at two public universities in the UK for encouraging people to have accounts on the *Trusty* OSN platform. Therefore, all accounts except three testing accounts on the *Trusty* are real world users' accounts.

All activities in the *Trusty* social network have been stored in its database. In order to keep all the activities, which happen in the *Trusty*, nine tables have been created in the database, see Figure A.15. In the figure, *users* table was created to keep general information about users including id, first name, last name, email, password, reputation value, profile picture, remember token, and created and updated profile information. In this table, the dynamic value is the reputation value as it is mentioned in Chapter 6. Table *confidences* was created to keep users trust values in each others. This table data is dynamic since trust values (defined in Chapter 6) are dynamic values. The trust values are updated when a user has the owner role in a co-owner data sharing process. The *notifications* table keeps information about posts including *post-id, user-id, click, and read*. Table *post-tags* was designed to keep information about posts on the *Trusty*. Tagged users' ids and post ids, which users were related to, are kept in the *post-tags* table. *Friends* was created to keep, who is friend with whom, with users' ids. Table *post-securities* was created to keep users' *CIAPP* choices and *Alternatives choices* on a post. The *posts* table was created to keep all information about a post. The post type (*i.e. texts, photos, videos, etc.*), who posted the post, who was tagged on the post, what is fuzzy decision and what is group decision, is it shared/ not shared, what is the sensitivity value for the post, in which round the consensus is reached by the group, is the shared post controlled for re-sharing flow, all

these information have been kept in the *posts* table. The table *results* was created to keep the trust loss and trust gain values for each owner in a co-owned post. The last table is *questions* which was created to keep results of two questionnaires that have been used to evaluate the *Trusty* network.

Figure A.16 shows a screenshot from Trusty database which includes details of shared co-owned data contents. The most useful and related information from the figure are as follows; number of co-owners, the group's decision, the number of the rounds which were taken to make a consensus-reached group decision, the sensitivity value, and the confidence in the targeted group. In the figure, *criteria* column gives information about whether all co-owners, whose ids are included to the post, give their choices on the alternative set and the *CIAPP* security features. 0 means co-owners not completed yet giving their choices on sharing process while 1 means all co-owners finish/ complete giving their choices.

Figure A.17 shows related information to a post in *Trusty* database. In the figure, all choices are made by co-owners and owners on a post are shown. For example, *CIAPP* security features choices and x_1, x_2, x_3, x_4 are saved in *Trusty* database. The sensitivity value of a shared co-owned data is also kept in this table. *round* is used to present in how many rounds co-owners were able to get the consensus in the sharing process.

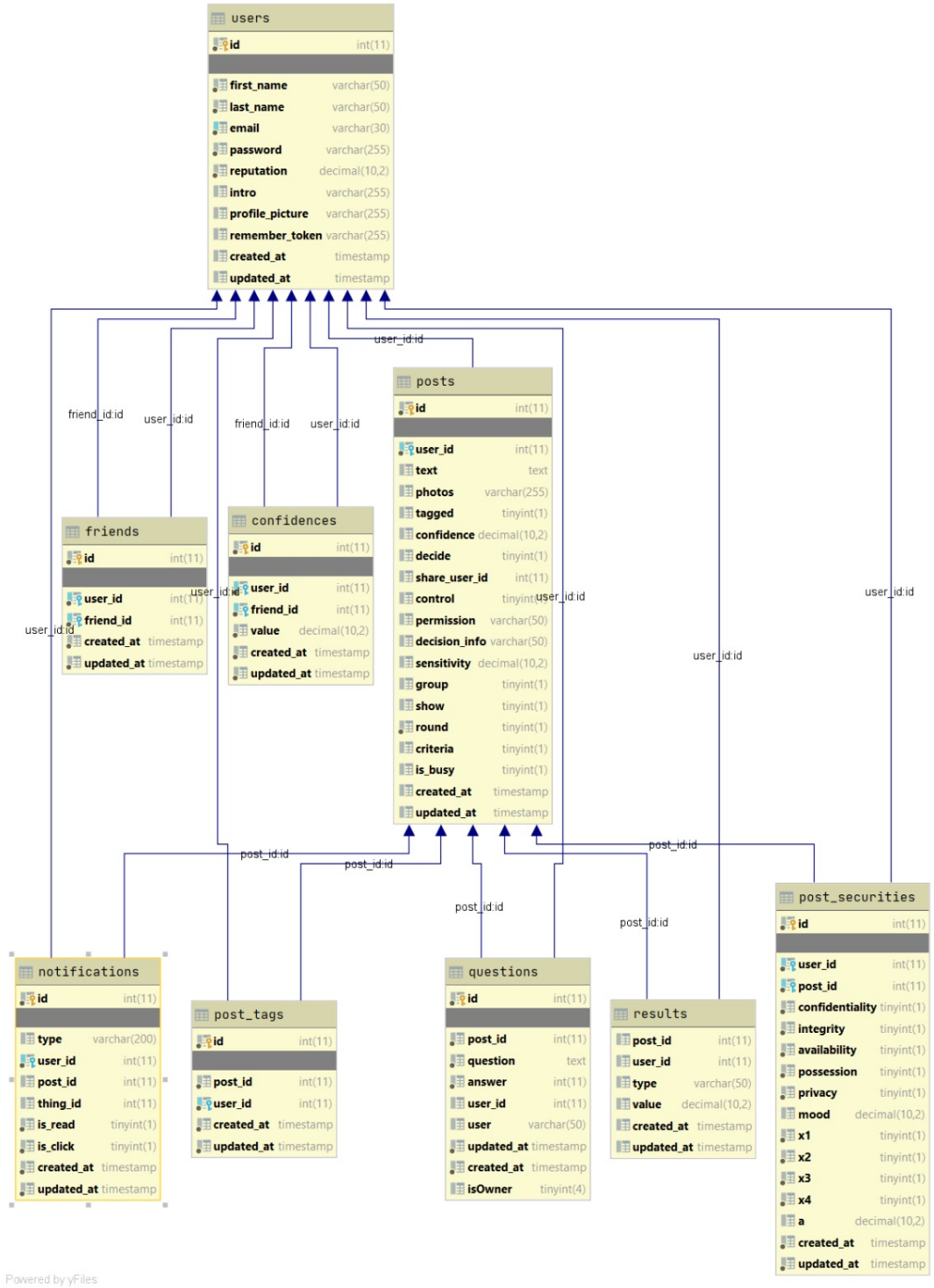

Figure A.15: Tables in *Trusty* Network Database

id	user_id	text	photos	share_use	control	tagged	confidenc	decide	permissio	decision_	sensitivity	group	show	round	criteria	is_busy	cretaed_a	updated_at
31	60024	[redacted]	http://ww	0	0	1	0.58	1	fullPermis	notReach	0.5	0	1	2	1	0	########	########
32	60026	[redacted]	NULL	0	0	1	0.5	1	notShare	notReach	1	0	1	2	1	0	########	########
33	60028	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
34	90028	[redacted]	http://ww	0	0	1	0.87	1	fullPermis	notReach	0.4	0	1	2	1	0	########	########
35	90054	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
36	90051	[redacted]	http://ww	0	0	1	0.8	1	notShare	notReach	1	1	1	2	1	0	########	########
37	90044	[redacted]	http://ww	0	0	1	NULL	0	fullPermis	NULL	NULL	0	0	1	1	1	########	########
38	90044	[redacted]	http://ww	0	0	1	0.85	1	noPermis	notReach	0.6	0	1	2	1	0	########	########
39	90044	[redacted]	http://ww	0	0	1	0.86	1	noPermis	notReach	0.55	0	1	2	1	0	########	########
40	90049	[redacted]	NULL	0	0	1	0.88	1	restricted	notReach	0.6	0	1	2	1	0	########	########
41	90026	[redacted]	NULL	0	0	1	0.77	1	fullPermis	notReach	0.5	0	1	2	1	0	########	########
42	90054	[redacted]	NULL	0	0	1	0.75	1	fullPermis	notReach	1	0	1	2	1	0	########	########
43	90054	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
44	90051	[redacted]	NULL	0	0	1	0.8	1	fullPermis	notReach	1	0	1	2	1	0	########	########
45	90027	[redacted]	NULL	0	0	1	0.6	1	notShare	notReach	0.8	0	1	2	1	0	########	########
46	90038	[redacted]	NULL	0	0	1	0.88	1	notShare	notReach	0.4	0	1	2	1	0	########	########
47	90041	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
48	90041	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
49	90045	[redacted]	http://ww	0	0	1	0.85	1	noPermis	notReach	0.6	0	1	2	1	0	########	########
50	90060	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
51	90056	[redacted]	NULL	0	0	1	0.88	1	notShare	notReach	0.2	0	1	2	1	0	########	########
52	90056	[redacted]	NULL	0	0	1	0.52	1	fullPermis	notReach	0.8	0	1	2	1	0	########	########
53	90057	[redacted]	http://ww	0	0	1	0.8	1	fullPermis	notReach	0.4	0	1	2	1	0	########	########
54	90059	[redacted]	NULL	0	0	1	0.67	1	fullPermis	notReach	1	0	1	2	1	0	########	########
55	90059	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########
56	90052	[redacted]	NULL	0	0	1	1	1	fullPermis	fullPermis	0	0	1	1	1	0	########	########

Figure A.16: Trusty Database

id	userid	postid	confidentiality	integrity	availability	possession	privacy	mood	x1	x2	x3	x4	a
51	60028	31	1	0	0	1	1	0.88	-3	-3	-2	3	0.88
52	60026	31	1	0	0	0	1	0.16	-3	-3	-2	3	0.16
54	60024	32	1	1	1	1	1	0.88	-3	-3	-3	4	0.88
55	60024	33	0	0	0	0	0	1	2	2	0	0	1
58	90027	34	0	1	1	0	0	0.46	-2	-2	-2	3	0.46
59	60024	34	0	1	1	0	0	0.28	-3	-2	0	2	0.28
60	90052	35	0	0	0	0	0	0.98	3	3	0	0	0.98
61	90050	35	0	0	0	0	0	0.99	2	2	0	0	0.99
64	90050	36	1	1	1	1	1	0.04	-4	-4	2	4	0.04
65	90049	36	1	1	1	1	1	0.02	4	4	2	2	0.02
70	90048	38	1	1	1	0	0	0.39	-4	-4	-2	3	0.39
71	90047	38	0	1	1	1	0	0.46	-3	-3	-1	3	0.46
72	90046	38	0	1	1	1	0	0.45	-2	-3	-1	3	0.45
73	90045	38	0	1	1	1	0	0.39	-3	-3	-2	3	0.39
78	90048	39	1	0	0	0	1	0.02	-4	-4	2	3	0.02
79	90047	39	1	1	0	0	1	0.08	-4	-3	3	4	0.08
80	90046	39	1	1	0	0	1	0.02	-4	-3	3	4	0.02
81	90045	39	1	1	0	0	1	0.03	-4	-4	3	4	0.03
84	90051	40	1	1	0	0	1	0.15	-3	-2	2	3	0.15
85	90050	40	1	1	0	0	1	0.23	-3	-3	2	3	0.23
88	90028	41	1	1	1	0	0	0.2	-3	-3	0	4	0.2
89	90031	41	1	1	0	0	0	0.22	-3	-3	0	3	0.22
91	90050	42	1	1	1	1	1	0.03	-4	-2	1	4	0.03
92	90049	43	0	0	0	0	0	0.91	3	3	0	0	0.91
94	90052	44	1	1	1	1	1	0.05	-3	-3	0	3	0.05
96	90026	45	1	1	1	1	0	0.04	-3	-3	0	3	0.04
98	90039	46	1	0	0	0	1	0.34	-3	-3	0	4	0.34
99	90042	47	0	0	0	0	0	0.97	4	3	0	0	0.97
100	90043	48	0	0	0	0	0	1	3	3	0	0	1
102	90046	49	1	1	1	0	0	0.29	-2	-2	2	3	0.29
103	90055	50	0	0	0	0	0	0.99	2	2	0	0	0.99

Figure A.17: Information Related to Posts in Trusty Database